PX 87

Message

_____

From: Ryan Zagone ████████@ripple.com]
Sent: 6/24/2015 2:09:52 PM
To: ████████████████████████████ripple.com>]
Subject: Fwd: Ripple Labs response to ████ request
Attachments: ████Final_RL_Response.pdf

---------- Forwarded message ----------
From: ████████████████ @ripple.com>
Date: Wed, Jun 24, 2015 at 3:59 PM
Subject: Ripple Labs response to ████ request
To: ████████████████████████.com
Cc: Patrick Griffin <████████ @ripple.com>, Phil Rapoport ████ @ripple.com>, ████████████████
<████ @ripple.com>, Antoinette O'Gorman <████████ @ripple.com>

Hi ████

Please find our full response to your list of questions attached. The 8 appendices contain relevant documents for many of the questions, and they are referred to in the respective answers.

As noted in the document, all material and answers are privileged and confidential, and subject to attorney-client privilege and attorney work product doctrine. The content in the document does not constitute legal advice

Please let us know if you have any questions or would like more information.

Regards,

████

Ripple Labs Inc
Markets and Trading
████████
www.ripple.com   www.ripplelabs.com

Ripple Due Diligence Questions and Document Request List (06.24.15)

Corporate Governance Structure

1. **Articles of incorporation and bylaws**

Please see appendix 1.

2. **Provide organizational charts for the following:**
   a. **All legal entities, including any non-US subsidiaries**
   b. **Board of directors and committee structure**
   c. **Advisory Committee**
   d. **Senior Management Team and committee structure**
   e. **Legal and Compliance Group**

Please see appendix 2.

3. **Identify and describe investors with $\geq 5\%$ interest**

Please see appendix 3.

Financial Information

4. **Provide financial information including balance sheet and income statement (audited if available).**

Please see appendix 4.

5. **Describe Ripple's business model.**

Ripple is an open-source protocol that exists as a public good. It is not owned by anyone. Ripple Labs, as a supporter of the Ripple protocol, provides professional services and a suite of closed-source software products that enable seamless integration with the protocol.

Ripple Labs' primary business consists of (1) professional services related to business use cases development, technology deployment and systems integration; and (2) building and licensing software to help financial institutions interact with the protocol.

Additionally, Ripple Labs has XRP holdings – the digital asset within Ripple – which may appreciate in value with increased use of the protocol.

6. **Describe how Ripple generates revenues (is it through fees or by making markets)?**

Ripple is an open-source protocol and does not generate revenues in and of itself.

1

Ripple Labs generates revenues by providing professional services and products for connecting to Ripple, including integrations, licensing software and building custom applications for users

Trade Mechanics

7. **Walk through each element of a transaction and settlement process, including parties, flows, and systems used. Identify parties to each leg of the transaction and settlement process.**

Please see appendix 5.

8. **Provide sample trade flows.**

Please see appendix 5.

9. **Identify all products traded on the Ripple platform. Is this just spot?**

We are only discussing spot FX transactions for the purposes of ▮▮▮▮▮▮▮▮ s engagement with Ripple. Ripple Labs currently only supports spot FX transactions use-cases.

10. **Describe the transparency of bids, offers and traded prices.**

Bids and asks are placed in public order books and sorted by price. It is a fully transparent market.

a. **How does the matching engine work?**

The code is open-source and auditable, yet we do not yet otherwise have documentation prepared explaining the matching engine.

11. **Is Ripple a dark pool?**

No. Ripple is a "lit" trading venue

12. **Can ▮▮ specify who we get matched up with on trades?**

Not in all cases. As a market maker, ▮▮ controls the endpoint banks ("gateways") for which it wants to provide liquidity. The gateways in turn validate and authorize market makers. ▮▮ does not necessarily control which other market makers are authorized by the gateways. ▮▮ may be matched up with one of these unknown market makers in the order book. Unless ▮▮ requires the endpoint banks to disclose the identity of other participants, ▮▮ may not necessarily know the identity of other traders in the market (similar to how ▮▮ currently does not know the identity of every counterparty on a traditional exchange like NASDAQ).

13. **Can ▮▮ set credit limits?**

2

Yes. As a market maker, ▮ must explicitly specify the credit exposure it is willing to take with each counterparty. In Ripple, credit limits are established with "trust lines" that each entity makes with each of its counterparties. For example, ▮ may choose to hold up to $10mm USD issued by Citibank on Ripple. To do this, ▮ would initiate a trust line to Citibank establishing the currency and value limit. Citibank must authorize the trust line. Once approved, ▮ can revoke the trust line or change the limit in the future if desired.

14. Given that this is a pre-funded market, how does Ripple ensure that a counterparty's funds are locked up at the relevant bank?

Ripple Labs does not provide any assurance of creditworthiness of any participants. Participants should rely on their own due diligence. Also, Ripple does not necessarily have to be a prefunded market. For example, Citibank may choose to extend a credit line to ▮ This could enable ▮ to start with a $0 balance account and draw down against the credit line to deliver funds for payments.

a. How does ▮ know which correspondent banks to pre-fund?

This is ▮ s decision based on business needs of ▮ or its customers.

b. Who is at risk if a correspondent bank hasn't been pre-funded?

As mentioned above in 14, Ripple does not necessarily have to be prefunded. Balances issued by financial institutions are liabilities of those institutions. Most of these institutions are fractional reserve, so they are not inherently 100% "prefunded". Even if the bank requires 100% prefunding for Ripple market makers, there is still credit risk in many scenarios. If an endpoint ("gateway") bank defaults, the holders of its balances are at risk of potential loss. This risk can be accounted for in the funding and delivery quote posted by the market maker, just as is done today.

c. As the network grows, will clients that do not have a correspondent banking relationship with a Ripple gateway be allowed to transact? If so, do you anticipate any local market issues when a market opens and a number of movements in the local currency are contemplated?

We are confused by the meaning of the question. Gateway banks will provide proxy access to the Ripple network for their customers. The gateway bank – which can be either an existing correspondent bank or a respondent bank – controls who can or cannot use their service, just as an ACH-enabled bank today controls which customers are able to get proxy access to the ACH network to send payments.

15. How does one become a gateway bank and a market maker? What are the barriers to entry?

3

To become active on Ripple – as either a market maker or gateway – one would first create a Ripple account. Gateways and market makers are distinguished in how they use their account. A gateway issues balances into Ripple. (i.e. It has outstanding liabilities held by other participants on Ripple; it acts as a custodian.) What distinguishes a market maker is that it has relationships with multiple gateways and posts prices to buy and sell their balances.

As Ripple is an open protocol, there are no barriers to entry related to proprietary code or technology. Institutions simply integrate Ripple's open source code to participate.

Ripple does offer the ability for gateways to "authorize" accounts, which serves to create closed loop networks within the protocol. These are essentially networks of financial institutions, which can dictate their own rules and specific barriers to entry. This is the same functionality that exists with payment systems today. For example, the Federal Reserve and NACHA each have their own rule sets for their networks that use ACH. They decide whom to authorize as participants based on their own requirements, but each closed network exists on the same underlying technology. Meeting network-specific requirements would be an entry barrier if an institution was looking to join a network.

16. What is Ripple's on-going role in the platform, if any?

Ripple Labs is the primary contributor to the open and closed-source products that interface with Ripple. Ripple Labs plans to contribute code and products as long as FIs are willing to continue using our version of the software. Ripple Labs also provides professional services and engages in business development and regulatory outreach to build a compliant ecosystem around the protocol.

17. What is Ripple's role, if any, in the trade execution and settlement process?

Ripple Labs is a software and technology provider to financial institutions. Ripple Labs does not own or operate the Ripple protocol, but rather provides software solutions to help institutions integrate and use the technology. Ripple Labs would not have any anticipated role in trade execution or settlement. The financial institutions using the technology, along with the Ripple protocol itself, carry out these functions.

18. How are trades confirmed?

Trades are executed, fully settled, and confirmed in the instant that the ledger is updated Confirmation of a trade and the transfer of ownership are simultaneous and observable on the open ledger. Software that analyzes the ledger can provide notifications and generate reports based on this data as needed.

19. Reversibility – explain how trades are reversed and error trades are handled.

4

Transactions on the Ripple protocol are not reversible, the same as wire payments today. Rules between participants establish the circumstances when a payment should be returned, just as network rules function today. The returned transaction would just be another irreversible transaction in the opposite direction.

Reversing a transaction is not a function of the underlying settlement technology in Ripple or in today's existing payment rails The governance and rules that the participants agree to dictate when, how and why transactions can be returned. Participants in Ripple can opt to use current rules from existing networks or decide to establish new governance between counterparties. This decision is fully up to the participants.

20. Describe the role of XRP in transactions.

XRP has two functions: (1) a security mechanism that is mandatory for all users and (2) a bridge between fiat currencies that is entirely optional.

Ripple deploys a digital currency, called XRP, as a security mechanism. In this way, XRP is similar to a postage stamp for each transaction. All account holders on Ripple are required to hold a small reserve of XRP. A small fraction of an XRP is destroyed with each transaction (ex. $0.000001). The small portion of the XRP that is destroyed is not a fee collected by anyone, rather a cost of using the Ripple technology.

Under normal network volumes, this XRP cost remains very small. However, in the event that a participant tries to overwhelm the network with disruptive activity – for instance with a denial of service attack – the Ripple technology will exponentially increase the cost of each transaction. This feature aims to quickly bankrupt the bad actor of its XRP reserve, prohibiting any additional traffic from its account.

In this role, XRP blocks a denial of service attack from overwhelming the network, ensuring security and stability of the Ripple infrastructure at a minimal cost to users.

XRP's second and optional role is as a bridge currency. Participants on Ripple can make markets directly between fiat pairs (e.g. EUR/USD) without using XRP as an intermediary or bridge currency. But some market makers may choose to use XRP as a bridge currency in some scenarios if it is operationally beneficial to them.

a.   Does ▮▮▮ have to hold XRP to be a market maker in the network?

Yes, ▮▮▮ would need a small amount of XRP for its reserve account. A very small amount (e.g. $10 worth) would be plenty, and Ripple Labs would be happy to provide this free of charge. If

5

this is an issue, we may be able to devise a method where Ripple Labs custodies the XRP on behalf of ▮ This option would need to be discussed further if it is necessary.

       b. As a liquidity provider, when might ▮ need to provide liquidity in XRP?

▮ would never need to, but in some cases ▮ may want to. For example, ▮ may not have bank accounts in India, but a corporate client may want to send a payment to India. ▮ ould be unable to directly quote USD/INR, but ▮ could quote XRP/USD and another participant could quote XRP/INR. Ripple could bridge these two order books to synthetically create USD/INR liquidity. Use of XRP for this purpose is entirely optional.

       c. If MS has to provide liquidity in XRP or hold XRP, does ▮ ave to register with FinCEN as an MSB?

FinCEN's definition of MSB excludes "banks and foreign banks". Regulatory and compliance implications would be derived from ▮ existing bank licensing.

       d. Will market makers require any other licenses/registrations (e.g., NYDFS BitLicense)?

Licensing requirements may vary depending on the market maker's existing status as a broker-dealer, bank, etc., as well as the nature of the relationship with other market participants.

       e. How will you ensure that market makers have all required licenses/registrations?

Given that Ripple is an open protocol, Ripple Labs cannot provide assurances that market participants are properly licensed. Participants are empowered to limit their interaction on the network to known counterparties with whom they are comfortable transacting in a compliant way.

21. Ripple Ledger
       a. Explain how the Consensus Process works and its scalability.

Please see this link for more information: https://ripple.com/knowledge_center/the-ripple-ledger-consensus-process/

       b. Can you show us what the ledger looks like?

We provide a ledger explorer tool here: https://www.ripplecharts.com/#/graph There are other versions created by non-Ripple Labs developers as well.

22. Can ▮ trade outside the system and settle within the system? How would that work?

6

Two parties can agree to a trade and then send payments to one another. (E.g. ▮▮▮ sends counterparty $1.1mm, Counterparty sends ▮▮▮ €1mm). To achieve "payment vs. payment", it would require the use of a smart contract as escrow agent or the creation of a custom order book. In typical trades that occur on Ripple, payment vs. payment is the default.

Legal Framework

23. Provide copies of Ripple's Rulebook, Form Agreements, Disclaimers/Disclosures (including any disclosures to all clients/liquidity takers).

Please see appendix 6 for sample Integrator and Bank agreements.

24. In addition its MSB registration with FinCEN, identify any other state or federal licenses or registrations Ripple maintains or for which applications are pending.

Ripple Labs is in the process of registering a subsidiary as a money transmitter and a virtual currency business in New York State. We are reviewing with counsel the need to apply for licenses in other jurisdictions.

    a. Identify any non-US licenses or registrations.
    b. How have you gotten comfortable that you have all required licenses/registrations?

Ripple Labs will certainly apply for more licenses in other states such as California, Texas, Florida, etc. Ripple Labs has not yet determined the identity of all of the States in which it will seek to be licensed as a money transmitter.

25. Is XRP afforded protections similar to other currencies under the UCC?

Although we are not aware of statutory or case law on point, we expect that XRP would not be treated as a currency under Article 9 of the UCC, but rather as a "general intangible." That is the catchall classification of intangible assets, such as accounts, not otherwise classified. Assuming the UCC treats XRPs as general intangibles, ▮▮▮▮▮▮▮ would need to file a UCC financing statement in the location of the pledgor, typically the state of incorporation of organization.

We understand that there also may be an argument to treat XRP as a "financial asset" under Article 8 of the UCC, but we are not aware of any regulatory or judicial treatment of XRP as such to date. Under Article 8, lenders can perfect a security interest in an uncertificated financial asset, through a "control agreement" with the pledger.

We expect that future treatment of XRP and other virtual currencies by federal and state regulators and courts will impact this analysis, and we will structure the transactions on the basis of such treatment as it develops.

    RPLI_SEC 0095174

a. Would ▮▮ benefit from the binding nature of a trade executed on the Ripple Platform at the time of trade execution (the carveout to the Statute of Frauds for financial transactions)?

We expect that ▮▮▮▮▮ would benefit from the exception from the Statute of Frauds for qualified financial contracts for foreign exchange transactions effected using the Ripple protocol. Applicable states, including New York, California and Pennsylvania, do not require such contracts to be in writing to be enforceable, provided there is sufficient evidence that such contract has been made, and that the parties have signed a prior or subsequent written statement to be bound by the terms of a contract entered into by such means (i.e., electronic messages, telephonically, etc.).

26. In the event of a bankruptcy of a trade counterparty involving XRP, is the trade a qualified financial contract that benefits from the bankruptcy safe harbors?

Whether or not such agreements constitute securities contracts or transactions involving settlement payments is untested, and these transactions may not fall under the safe harbor protections of Section 546(e) of the Bankruptcy Code. However, from inception of the process through and including the payment of the funds at the conclusion of the process/transaction, ▮▮▮ should not be exposed to risk associated with counterparty insolvency or bankruptcy to the extent it acts as a mere conduit of the funds, transferred by the owner to the beneficiary. To the extent ▮▮▮▮▮ effects transactions as riskless principal, its counterparty risk could be mitigated by agreement with its counterparty financial institutions.

27. When does legal settlement/payment finality occur for currencies sent through the Ripple Network?

Legal finality of transactions in foreign exchange transactions typically occurs when the foreign exchange is recorded on the books and records of ▮▮ counterparty depository institution. We envision foreign exchange transactions effected by ▮▮ should settle on the books and records of such counterparties within a few minutes, in each case.

a. Do you have any legal opinions to this effect?

Because the details of these transactions have not been determined, and transactions involving virtual currencies are currently uncertain, we do not have legal opinions on point. As we further detail the transactions, we would be happy to work with you and competent counsel to obtain legal opinions where necessary or appropriate.

28. If trading anything other than deliverable spot on the Ripple Network, we will need to undertake Dodd Frank diligence (i.e., SEF registration, real time reporting, etc.)

8

Because we understand that only spot currencies (fiat and virtual) will be traded via the Ripple protocol, there should he no need for ████ to undertake additional due diligence regarding reporting and recordkeeping obligations under Dodd Frank. If there are additional, specific products that ██ is concerned with, we would be happy to address them.

29. If retail clients can use the Ripple Network, is Ripple a registered retail foreign exchange dealer?

Ripple Labs is not a registered retail foreign exchange dealer. The registration requirements for retail foreign exchange dealers arise when a person acts as counterparty or offers to act as counterparty to an off exchange transaction with a person who is not an eligible contract participant in either a foreign exchange derivative (e.g., futures contract, futures option contract, or options contract on foreign exchange); or a leveraged contract on foreign exchange. Because the foreign exchange transactions effected via the Ripple protocol do not fall into either of these categories, Ripple Labs does not need to register as a retail foreign exchange dealer.

a.   Can we limit our trading to institutional-only accounts?

Through contract, ██████████ should be able ensure that each counterparty to transactions on Ripple are eligible participants.

Compliance/BSA/AML/OFAC

30. Provide and inventory of all compliance related policies and procedures, on a legal entity basis.

Ripple Labs' general compliance-related P&Ps are as follows:

- Privacy Policy
- Code of Conduct
- Anti-Fraud Program

(If this does not fully satisfy the question, please let us know. We are unclear on the meaning of the question.)

31. Provide copies of BSA/AML/OFAC policies and procedures, on a legal entity basis.

Note: This request item is applicable to financial institutions subject to regulation under the Bank Secrecy Act. At this time, Ripple Labs, Inc. ("Ripple Labs") wholly owns two money services business ("MSB" or non-bank financial institution ("NBFI") subsidiaries — Ripple Trade, LLC and XRP II, LLC – both of which are subject to BSA/AML/OFAC regulation requirements.

RPLI_SEC 0095176

An inventory of relevant BSA/AML/OFAC Programs/Policies and implementing procedures for each Ripple MSB subsidiary is listed below. Applicable BSA/AML/OFAC Program documents are attached separately in appendix 7.

1. Ripple Trade LLC

Ripple Trade, LLC was formed on May 28, 2015 in response to a Settlement Agreement with regulatory authorities to move the Ripple Trade service into a money services business ("MSB") entity, registered with the U.S. Treasury's Financial Crimes Enforcement Network ("FinCEN")[1]. Ripple Trade registered with FinCEN as a money services business on June 2, 2015.

Ripple Trade BSA/AML/OFAC Program (see attached documents)

- BSA/AML/OFAC Program/Policy (approved June 12, 2015)
- Compliance and Oversight Committee Charter (approved and adopted June 12, 2015)
- BSA/AML/OFAC AML Training Program

Ripple Trade: Inventory of BSA/AML/OFAC Procedures (*available upon request*)

1- Customer On-boarding – (in draft)

Ripple Labs has developed a customer identification tool to assist with identification for Ripple Trade users. Onboarding procedures will be finalized once the tool is launched (end June 2015). New customer onboarding was suspended, effective June 2, 2015, until this functionality is in place. Customer identification and basic customer due diligence processes include automated non-documentary verification of Ripple Trade users, KYC in accordance with Ripple Trade's BSA/AML/OFAC AML Program requirements, screening against Office of Foreign Assets Control ("OFAC") sanctions lists, as well as screening to identify Politically Exposed Persons (PEPs).

2- OFAC Match Verification Procedures

Describes OFAC screening methodology, match verification logic, procedures for escalation, further investigation, OFAC reporting and potential SAR filing when true matches are identified.

3 - Monitoring, Investigations and SAR Guidelines (general)

Describes available investigation tools, general alert, monitoring, and investigations procedures, SAR filing and follow-up reviews, law enforcement inquiries, and record retention requirements.

4 – AML Transaction Monitoring Procedures – (in draft)

---

[1] In May 2015, Ripple Labs and its wholly owned subsidiary XRP II entered into a Settlement Agreement with the Department of Justice and FinCEN.

10

Production of monthly transaction monitoring reports will commence on July 1, 2015; related procedures will be finalized once report production begins.

5 - BSA e-filing Procedures
Describes BSA e-filing process, step-by-step SAR filing, and MSB registration renewal.

6 - Unusual Activity Reporting ("UAR") - Internal
Workflow and Ripple User Support procedures governing employee (internal) reporting of unusual activity to AML compliance staff for further investigation.

7 - Law Enforcement Inquiries Requests
General and desktop procedures governing response to law enforcement requests for information, receipt of subpoenas, NSLs, etc.

8 - 314(b) Request Procedures
Describes Ripple Trade's participation in FinCEN's voluntary information sharing program (registered on June 3, 2015), incoming and outgoing request and response procedures, information sharing confidentiality, and record retention requirements.

9 - External Review - Response Procedures
Procedures governing management and tracking of actions to address/resolve findings or issues resulting from independent audit reviews or regulatory examinations of Ripple Labs BSA/AML/OFAC Programs.

10 - Record Retention
Lists record type and record retention schedule.

---

2. XRP II, LLC
XRP II, LLC, a wholly owned subsidiary of Ripple Labs, Inc., is a FinCEN registered money services business (as of September 2013). XRP II engages in the sale and transfer of Ripple Labs' virtual currency, XRP, to third parties on a wholesale basis. All sales of XRP conducted by XRP II are for the benefit of Ripple Labs, its ultimate parent company, and represents one method by which Ripple Labs raises working capital.

XRP II BSA/AML/OFAC Program (see attached documents)
* BSA/AML/OFAC Program/Policy (last approved April 30, 2015)
* BSA/AML/OFAC AML Training Program (updated annually)

11

Inventory of BSA/AML/OFAC Procedures (*available upon request*):

1- Customer On-boarding
Step-by-step procedures describing XRP II's CIP and KYC processes for on-boarding new customers. Also describes XRP II's initial and ongoing OFAC and PEP screening processes.

2- OFAC Match Verification Procedures
Describes OFAC screening methodology, match verification logic, investigation and escalation processes, reporting to OFAC and potential SAR filing in instances of true match identification.

3 - Monitoring, Investigations and SAR Guidelines
Describes alert processes, investigation tools, general monitoring and investigations procedures, SAR filing and follow-up continued activity reviews, law enforcement inquiries, and record retention requirements.

4 - Transaction Monitoring Procedures (desktop)
Describes (manual) transaction monitoring conducted by AML Compliance staff (daily, monthly, quarterly monitoring), review process, and escalation procedures.

5 - BSA e-filing Procedures
Describes BSA e-filing process, step-by-step SAR filing, and MSB registration renewal.

6 - Law Enforcement Inquiries/Requests
General and desktop procedures governing response to law enforcement requests for information, subpoenas, NSLs, etc.

7 - 314(b) Procedures
Describes XRP II's participation in FinCEN's voluntary information sharing program under Section 314(b) of the USA PATRIOT Act, incoming/outgoing 314(b) request/response procedures, information sharing confidentiality, and record retention requirements.

8 - Unusual Activity Reporting ("UAR") - Internal
Workflow and Ripple User Support procedures governing employee (internal) reporting of unusual activity to AML compliance staff for further investigation.

9 - AML External Reviews - Response Procedures
Procedures governing management and tracking of actions to address/resolve findings or issues resulting from independent audit reviews or regulatory examinations of Ripple Labs BSA/AML/OFAC Programs.

10 - Record Retention Procedures
Lists record type and required retention schedule.

32. What types of entities are on the Ripple platform/can join the platform, e.g., HFT, retail?

12

Because Ripple is a decentralized, open-source ledger and payments network which allows users to transfer and exchange digital representations of currencies (including fiat and other decentralized digital) and commodities issued by network users, any person/entity can join.

The protocol also permits bilateral, real-time funds settlement. Ripple Labs provides integration services, among other things, for entities that wish to use the Ripple protocol.

The Ripple technology sits deep in the plumbing of the payments system, and is not intended to be something that large numbers of consumers interact with directly.

Since Ripple relates to funds settlement and not customer on-boarding, banks and other financial services providers integrating with or testing the Ripple protocol are able to do so while continuing to use the same systems and processes for CIP, CDD and EDD that they always have.

a. **What is the account opening process – KYC, EDD, expected account activity, source of funds, OFAC screening?**

This question is applicable to customers of Ripple Trade, LLC and XRP II, LLC (Ripple Labs' MSB subsidiaries). As non-bank financial institutions (NBFIs), both MSB subsidiaries are subject to BSA/AML/OFAC regulatory requirements. Customer identification, KYC, EDD, expected activity and source of funds requirements, and OFAC sanctions screening processes are described in the BSA/AML/OFAC Program governing each entity (relevant documents attached in appendices 7 and 8).

b. **What ongoing client due diligence process does Ripple undertake?**

As indicated in response to 31 above, due diligence is conducted on customers of Ripple Labs' regulated MSB entities: Ripple Trade and XRP II. Customer due diligence and enhanced due diligence processes are described in the BSA/AML/OFAC Program governing each entity (refer to attached Ripple Trade and XRP II Program documents in appendix 7).

33. Transaction monitoring

a. **Describe internal controls and processes in place to monitor transaction activity for potentially suspicious activity, economic sanctions (OFAC), Funds Transfer and Funds Transfer Rules**

Due to the relatively low number of transactions and customers of XRP II, transaction activity is manually monitored by AML Compliance staff members on a daily, weekly, monthly and quarterly basis.

Ripple Trade, LLC has developed and is in the process of implementing transaction-monitoring scenarios to alert on funds sent to or from Ripple Trade users. Specifically, Ripple Trade has developed monitoring scenarios to identify:

- █████████████████████████████████████

13
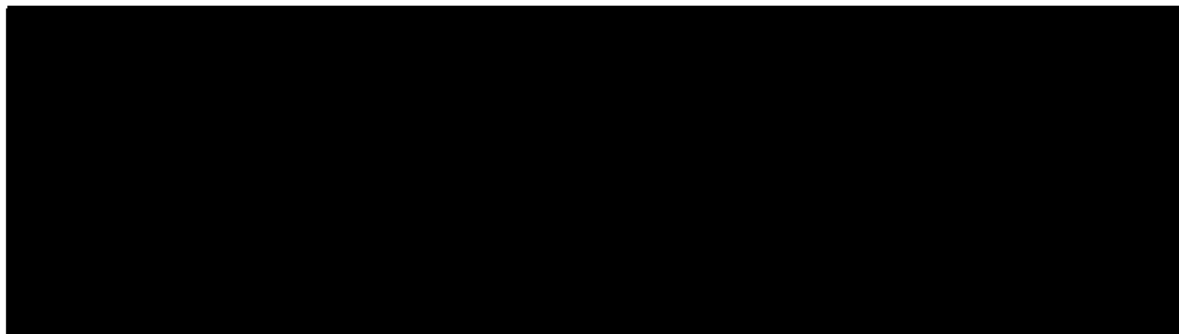
Monthly reporting will commence on July 1, 2015. Ongoing evaluation of report output may result in the development of additional transaction-monitoring scenarios.

Recent enhancements to Ripple Labs' global dynamic risk and analytical tools will further facilitate monitoring and investigation of suspicious transaction activity, transaction counterparty identification, flow of funds reporting, and degrees of separation reporting across the entire Ripple protocol.

> **b. Describe Ripple's Suspicious Activity Reporting process and controls, including any recent enhancements.**

For detailed description, please refer to the separate attachment titled *"Monitoring Investigations SAR Guidelines"* in appendix 7. Both MSB entities - Ripple Trade, LLC and XRP II, LLC - are subject to suspicious activity reporting (SAR) requirements in accordance with BSA reporting regulations.

> **34. Provide a detailed description of the implementation, completion and outstanding work related to implementing the Remedial Framework agreed to between Ripple Labs, XRP II and FinCEN.**

Refer to separate attachment *"Settlement Agreement — Remedial Measures"* in appendix 8.

> **35. Is Ripple subject to any ongoing state or federal investigations by law enforcement or other regulatory agency?**

No.

> **36. Identify any material pending state or federal litigation.**

None at this time.

Network and Protocol Security/Confidentiality and Privacy

> **37. Who holds/secures public and private key information?**

14

Each user of the Ripple network is responsible for securing his/her private key. Private keys can be hosted by a gateway or other institution. Public keys are publicly visible by design and do not need to be secured.

38. How is the Ripple protocol secured?

The protocol itself is continuously validating transactions through a network of secured servers reaching consensus. Ripple Labs controls who has access to modify official versions of the Ripple server code. Additionally, Ripple Labs is not aware of any incidents involving a loss of user funds due to insecure download of Ripple server software.

39. Describe the "integration" of the bank's account ledger into the Ripple Network.

On a high level, integration entails synchronizing the bank's GL with the Ripple ledger. When a balance is issued on Ripple, it must be immobilized in the GL to avoid a duplication of liabilities The GL must also "listen" for transactions that happen on the Ripple ledger to adjust the GL to reflect the appropriate changes in ownership that occur on the Ripple ledger. Ripple Labs provides closed source software to financial institutions to simplify the integration process.

40. What assurances will ██████ have regarding the confidentiality of its trades/settlements through the Ripple Network?

The Ripple network (and more broadly, all major blockchain technologies known to us) are inherently public, meaning that anyone can choose to run a network node and download and view a copy of the ledger. The Ripple ledger is pseudonymous, meaning that participants are identified by alphanumeric strings (e.g. rEsIsy2S4oV89jPrwyAf8CBF6pHtXL6fsl). The actual identity of the party controlling the account is not known to network participants. It is the responsibility of the user to keep their identity confidential. There are no assurances of confidentiality when using the Ripple network.

15

Appendix 1 — Articles of Incorporation

A0747403

35056635

CERTIFICATE OF AMENDMENT
OF THE
ARTICLES OF INCORPORATION
OF
OPENCOIN INC.
a California corporation

FILED
SECRETARY OF STATE
STATE OF CALIFORNIA

OCT 18 2013

The undersigned does hereby certify as follows:

FIRST: That the undersigned are the duly elected and acting President and Secretary of OpenCoin Inc. (the "***Corporation***"), a corporation organized and existing under the California General Corporation Law (the "***CGCL***");

SECOND: That in accordance with Sections 905 and 907 of the CGCL, Article 1 and Article 3 of the Articles of Incorporation of the Corporation are hereby amended to read in their entirety as follows:

"ARTICLE 1. NAME

The name of this corporation is Ripple Labs Inc."

"ARTICLE 3. SHARES

This corporation is authorized to issue only one class of shares of stock; and the total number of shares which this corporation is authorized to issue is Fifteen Million (15,000,000) shares of common stock, with a par value of $0.0001."

THIRD: That the foregoing amendment has been approved by the board of directors of the Corporation in accordance with Sections 307 and 902 of the CGCL;

FOURTH: That the foregoing amendment has been approved by the required vote of the shareholders in accordance with Sections 152, 603, 902 and 903 of the CGCL;

FIFTH: That the total number of outstanding shares entitled to vote with respect to the foregoing amendment was 9,082,400 shares of Common Stock;

SIXTH: That the affirmative vote of holders of not less than a majority of the outstanding shares of Common Stock was required to approve the foregoing amendment; and

SEVENTH: That the number of shares of each class voting in favor of the foregoing amendment equaled or exceeded the vote required.

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

79435-0002/LEGAL27740228.2

RPLI SEC 0095184

The undersigned hereby further declare and certify under penalty of perjury under the laws of the state of California that the facts set forth herein are true and correct of the own knowledge of the undersigned, and that this certificate is the act and deed of the undersigned.

Executed in Palo alto, California this 16th day of october , 2013

By: _____
    Chris Larsen, President

By: _____
                        Secretary

I hereby certify that the foregoing
transcript of _____ page(s)
is a full, true and correct copy of the
original record in the custody of the
California Secretary of State's office.

OCT 2 9 2013

Date: _____

DEBRA BOWEN, Secretary of State

CERTIFICATE OF AMENDMENT
TO
ARTICLES OF INCORPORATION
OF
NEWCOIN, INC.

The undersigned certifies that:

  1. She is the sole incorporator of NewCoin, Inc, a California corporation (the "*Corporation*"), and as such, constitutes a majority of the incorporators of the Corporation.

  2. That the Articles of Incorporation of the Company were originally filed with the Secretary of State of the State of California on September 19, 2011.

  3. The Corporation has issued no shares, and the incorporator adopts the amendments set forth herein.

  4. Directors were not named in the original articles of incorporation of the Corporation and have not been elected.

  5. That pursuant to Chapter 9 of the California Corporations Code, Article 1 of the Articles of Incorporation of the Company is hereby amended to read in its entirety as follows:

"ARTICLE 1: NAME

The name of this corporation is OpenCoin Inc."

The undersigned declares this 3rd day of October, 2012 at Palo Alto, CA under penalty of perjury under the laws of the state of California that she has read the foregoing certificate and knows the contents thereof and that the same is true of his own knowledge.

I hereby certify that the foregoing
transcript of _____ page(s)
is a full, true and correct copy of the
original record in the custody of the
California Secretary of State's office.

OCT 0 8 2012

Date _____

DEBRA BOWEN Secretary of State

ARTICLES OF INCORPORATION

OF

NEWCOIN, INC.

The undersigned, as incorporator of a corporation under the General Corporation Law of California, adopts the following Articles of Incorporation.

ARTICLE 1. NAME

The name of this corporation is NewCoin, Inc.

ARTICLE 2. PURPOSES

The purpose of this corporation is to engage in any lawful act or activity for which a corporation may be organized under the General Corporation Law of California other than the banking business, the trust company business or the practice of a profession permitted to be incorporated by the California Corporations Code.

ARTICLE 3. SHARES

This corporation is authorized to issue only one class of shares of stock; and the total number of shares which this corporation is authorized to issue is Ten Million (10,000,000) shares of common stock, with a par value of $0.0001.

ARTICLE 4. AGENT FOR SERVICE OF PROCESS

The name of the initial agent for service of process in the State of California is Corporation Service Company which will do business in California as CSC-Lawyers Incorporating Service.

ARTICLE 5. LIMITATION OF DIRECTOR LIABILITY

The liability of the Directors of this corporation for monetary damages shall be eliminated to the fullest extent permissible under California law.

91004-2110.0003/LEGAL17962258.1

ARTICLE 6. INDEMNIFICATION

This corporation is authorized to provide indemnification of agents (as defined in Section 317 of the General Corporation Law of California), whether by bylaw, agreement, or otherwise, in excess of the indemnification otherwise permitted in Section 317 of the General Corporation Law of California, subject only to the applicable limits set forth in Section 204 of the General Corporation Law of California with respect to actions for breach of duty to this corporation and its shareholders.

[Remainder of Page Intentionally Left Blank]

91004-2110.0003/LEGAL17982258.1

RPLI_SEC 0095190

IN WITNESS WHEREOF, the undersigned incorporator has executed these Articles of Incorporation on September 17, 2012.

91004-2110.0003/LEGAL17982258.1

I hereby certify that the foregoing
transcript of _____ page(s)
is a full, true and correct copy of the
original record in the custody of the
California Secretary of State's office

SEP 1 9 2012

Date: _____

DEBRA BOWEN, Secretary of State

Appendix 2a — Legal Entities
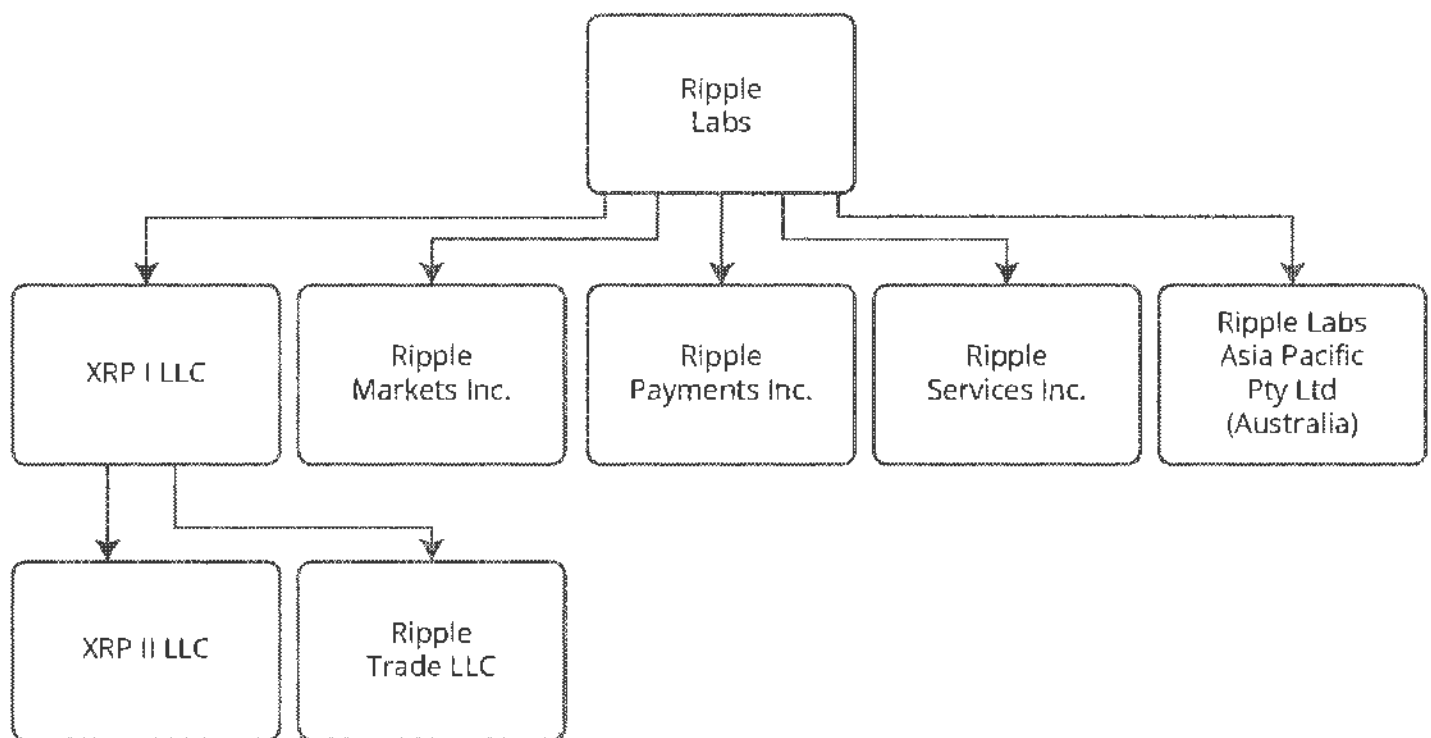
Appendix 2b — Board of Directors

Board of Directors Ripple Labs, LLC

Chris Larsen
David Schwartz
Susan Athey
Doug Chertok
Arjan Schutte
Bob Gunderson
Li Feng

Appendix 2c — Board of Advisors

Ripple Labs, LLC Advisory Board

- Osama Bedier
- Benjamin Cohen
- Donald Donahue
- Karl-Theodor zu Guttenberg
- Anja Manuel
- Saurabh Narain
- Alan Safahi
- Marcy Simon
- D.A. Wallach

https://www.ripplelabs.com/advisors/

Appendix 2d — Senior Management Team

Chris Larsen
President & CEO

CTO

Head of Regulatory
Relations

Chief Risk Officer

General Counsel

Brad Garlinghouse
COO

Patrick Griffen
**EVP of Business
Development**

Monica Long
**VP of Marketing
and Communications**

Controller

Asheesh Birla
VP of Product

VP of Delivery
and Integration

VP of Engineering

Antoinette O'Gorman
**Chief Compliance
Officer**
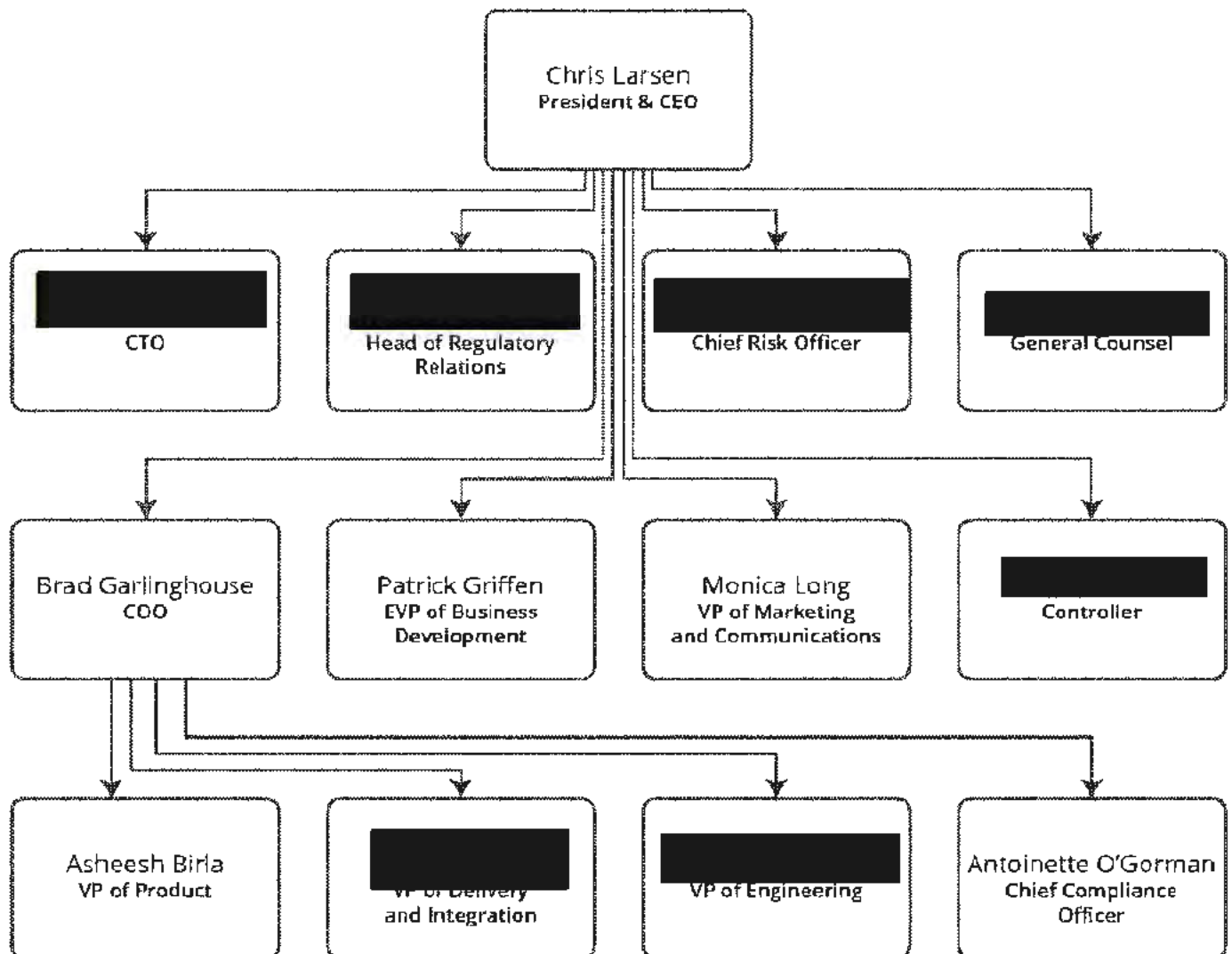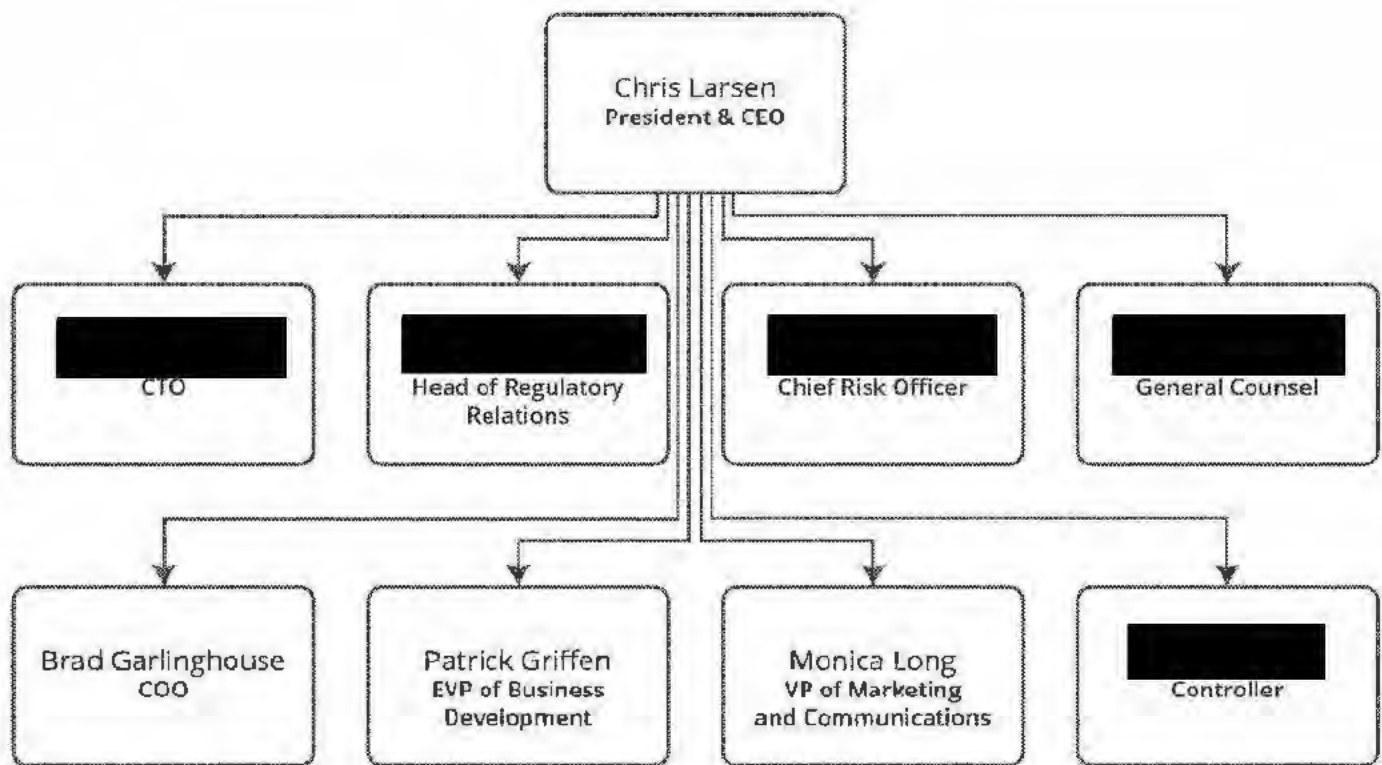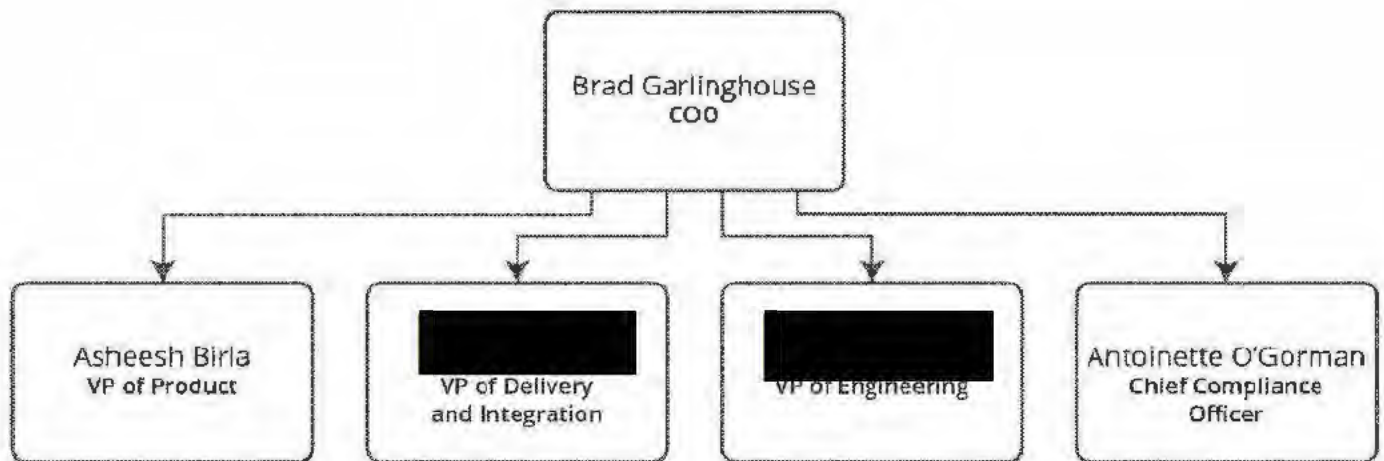
Appendix 2e — Legal and Compliance Group
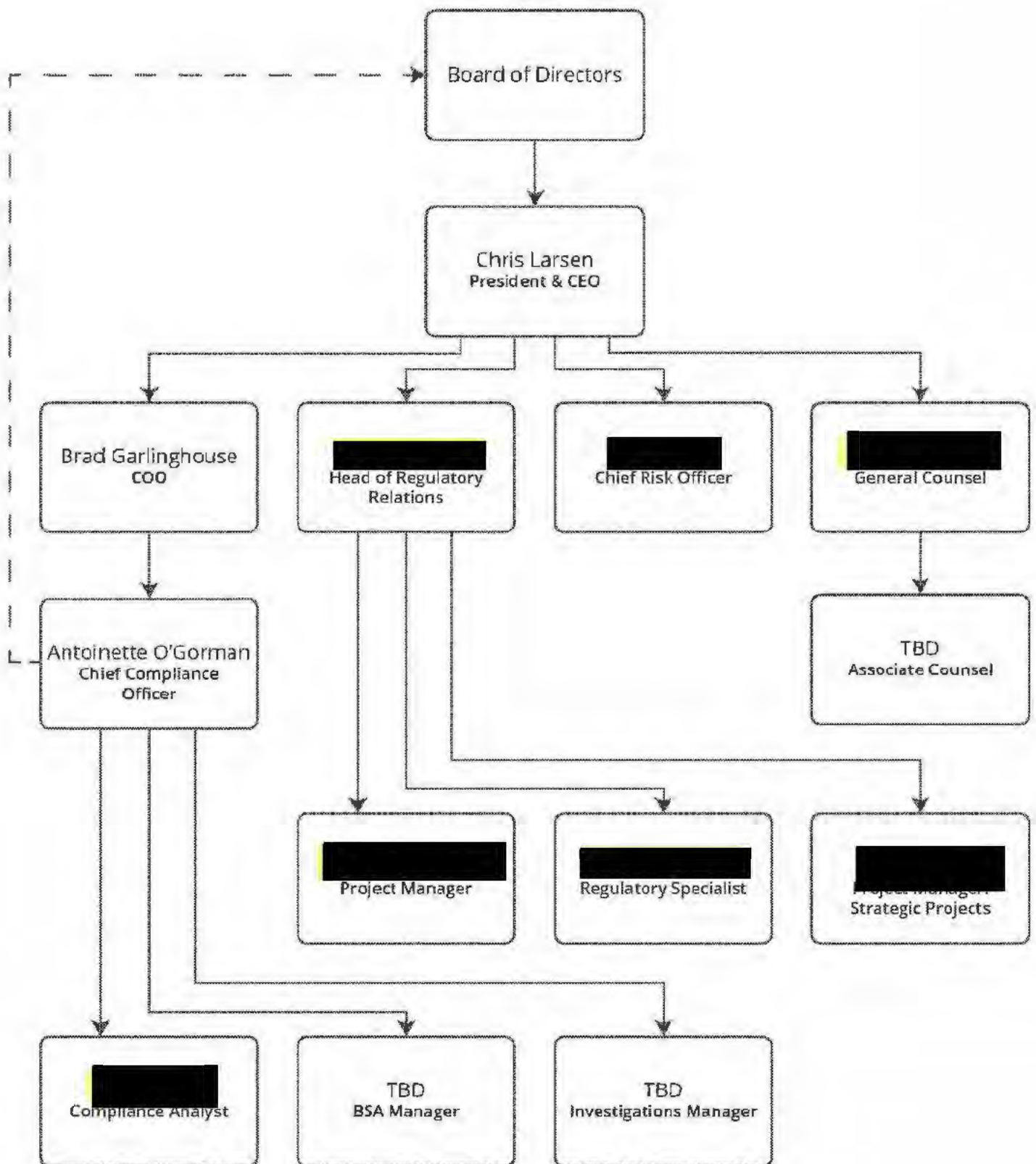
Appendix 3 — Investors with 5% of Interest or Greater

Investors with ≥ 5% interest

Name/ Company	Percentage of Interest
██████████████████████	5.20%
██████████████████████	24.43%
██████████████████████	6.94%

Appendix 4 — Financial Information

	Q4'14
Ordinary Income/Expense	
Revenue	
Integration Services Revenue	
XRP wholesale revenues	14,907,393
XRP Payroll Revenue	
XRP Vendor Revenues	
Total Revenue	
Total Cost of Revenues	
Operating Expenses	
Salaries & Benefits	
Contractors - Independent	
Facilities	
General Office & Other	
Travel & Entertainment	
Professional Services	
Sales & Marketing	
Software & Depreciation	
Total Operating Expenses	
Net Ordinary Income	
Other Income/Expense	
Interest Income	
Interest and Other Expenses	
Income Tax Expense	
Net Other Expense	
NET INCOME	

ASSETS	December 31, 2014
Current Assets	
Cash & Cash Equivalents	
Operating Cash (USD)	
Restricted Cash (USD)	
Bitcoin Holdings (BTC)	
Total Cash & Cash Equivalents	
Accounts Receivable	
Prepaid Expenses	
Total Current Assets	
Fixed Assets	
Other Assets	
TOTAL ASSETS	
LIABILITIES AND EQUITY	
Liabilities	
Current Liabilities	
Accounts Payable	
Accrued Liabilities	
Total Current Liabilities	
Total Liabilities	
Equity	
Common Stock	
Preferred Stock	
Retained Earnings	
Total Equity	
TOTAL LIABILITIES AND EQUITY	

Appendix 5 (Q7/8) — Transaction Elements and Trade Flow
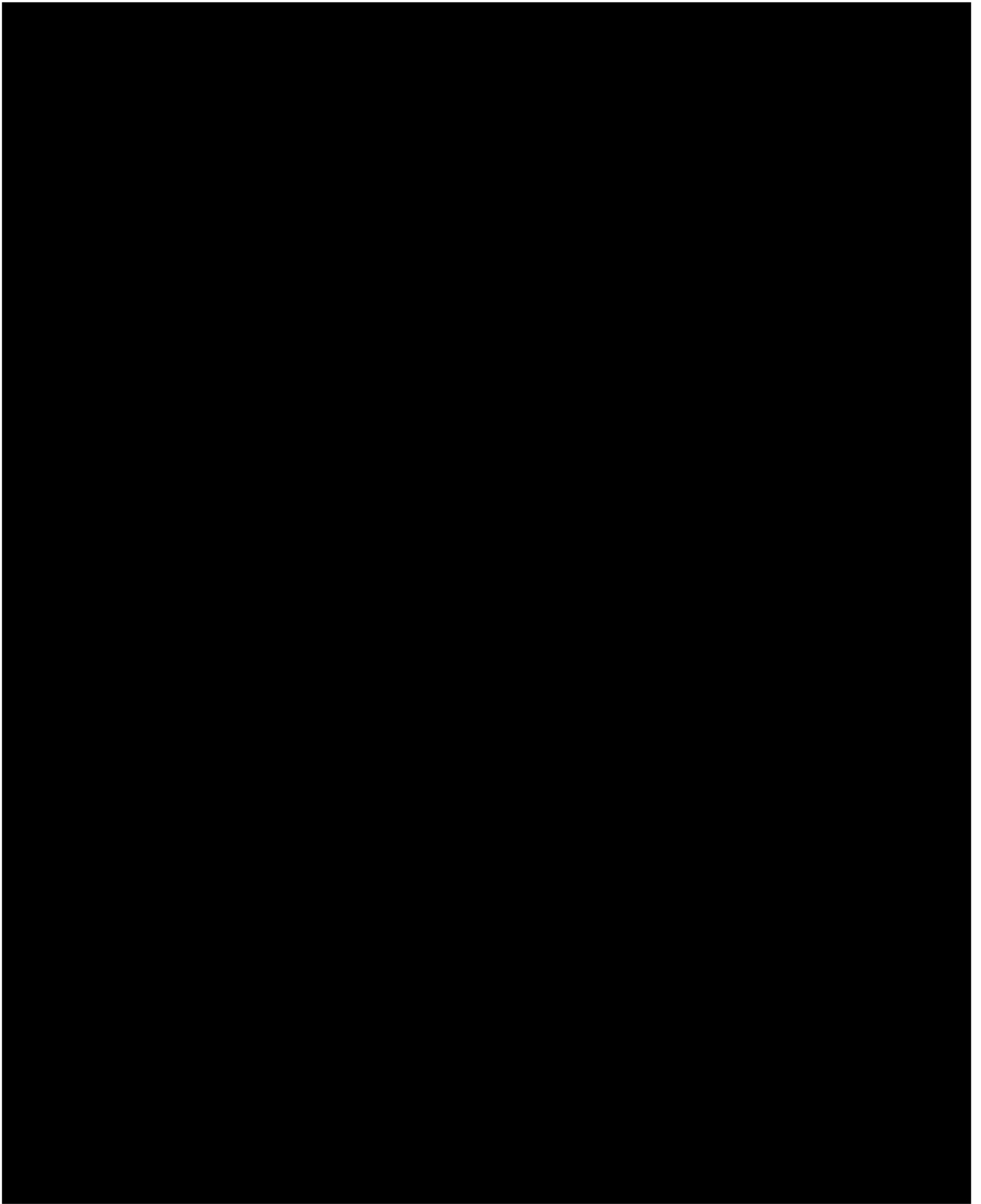
Appendix 6 (Q23) — Integrator and Bank Agreements

rippleLabs

INTEGRATION AGREEMENT

This Integration Agreement (the "**Agreement**") is entered into as of March __, 2015 (the "**Effective Date**") by and between Ripple Labs, Inc., a Delaware corporation ("**Ripple Labs**"), **Ripple Services, Inc.**, a Delaware corporation ("**Ripple Services**" and together with Ripple Labs, "**Ripple**"), and [Integrator] ("**Integrator**"). Ripple and Integrator are each referred to hereinafter as a "**Party**" and collectively as the "**Parties.**"

RECITALS

Ripple Labs has developed the Ripple Protocol and related technology to create a distributed Network that permits currency exchange and fund transfers. Ripple Services provides custom implementation, development and support services for settlement and exchange solutions using the Ripple Protocol. Integrator provides consulting, development and implementations services to its clients. Integrator is interested in integrating its and its Client's software with Ripple Software and related Ripple Technology (both terms as defined below) and providing access to such Integrated Solutions (as defined below) to clients. Ripple Labs has agreed to license Integrator to use the Ripple Software and Ripple Technology to develop and commercialize the Integrated Products as provided herein. The Parties wish to further set forth the terms under which Ripple Services will provide consulting and other services to support the Integrated Solutions and Integrator's efforts hereunder. Finally, the Parties wish to set forth the terms under which they will work together to promote the Integrated Solutions and their respective products and services.

NOW, THEREFORE, in consideration of the mutual covenants and agreements hereinafter set forth, the Parties do hereby agree as follows:

1.   **Definitions**

        1.1   "**Affiliates**" of an entity mean any corporation, company or other entity controlled by, controlling, or under the common control with such entity. For purposes of this definition, "control" means the direct or indirect ownership of more than fifty percent (50%) of the shares of the subject entity entitled to vote in the election of directors (or, in the case of an entity that is not a corporation, for the election of the corresponding managing authority) more than fifty percent (50%) interest in the income of such entity.

        1.2   "**Client**" means a person, company or other legal entity (i) for whom the Integrated Solution is used by Integrator on such Client's behalf, or (ii) to whom the Integrated Solutions is marketed, offered or made available by Integrator either as a product and/or as a service for the Client to use.

        1.3   "**Confidential Information**" has the definition set forth in Section 8.1.

        1.4   "**Derivative**" means, with respect to a party's Technology, any translation, modification, upgrade, customization, enhancement, adaptation, improvement, compilation, abridgment or other form in which an existing work may be recast, transformed or adapted, including a derivative work, and any material derived from or improving upon existing trade secret material or Technology.

        1.5   "**Documentation**" means instructions, technical data, specifications, administration and other documentation, including without limitation written comments and programmer

1

RPLI_SEC 0095213

rippleLabs

documentation, flow charts, logic diagrams, pseudo code, notations and other writings supporting the applicable Technology.

1.6 **"Intellectual Property Rights"** means patent rights, design rights, mask work rights, copyrights, trade secret rights, and any other form of protection afforded by law to inventions, models, designs, works of authorship, databases or technical information and applications therefor.

1.7 **"Integrated Solutions"** means the application(s) and/or product(s) developed in connection this Agreement which is created by combining, integrating or embedding the Ripple Software with any Integrator Product(s), whether offered or provided by Integrator to Clients in the form of a product and/or as a service. The use of plural "Integrated Solutions" versus singular "Integrated Solution" shall have no interpretive significance.

1.8 **"Losses"** means losses, damages, penalties, demands, judgments, expenses and costs of any kind whatsoever, including reasonable attorneys' fees and expenses.

1.9 **"Integrator Products"** means the software, hardware, services and other Technology of Integrator or its Clients, as well as the Intellectual Property Rights therein or related thereto.

1.10 **"Integrator Software"** means the software of Integrator or its Clients (and related Documentation) with which the Ripple Technology will be used as set forth in a Statement of Work.

1.11 **"Integrator Technology"** means any Technology developed, acquired or licensed by Integrator or its Clients, including Integrator Developed Technology, Integrator Background Technology and Integrator Derivative Technology (as such terms are defined in Section 5).

1.12 **"Ripple API"** means the application programming interface library that facilitates access to the Ripple Protocol and Ripple Network and that may be used to develop the Integrated Solutions.

1.13 **"Ripple Products"** means the software, hardware, services and other Technology made available by Ripple to Integrator or Clients, including the Ripple Software, Ripple Protocol and access to the Ripple Network, as well as the Intellectual Property Rights therein or related thereto.

1.14 **"Ripple Software"** means the Ripple Protocol, Ripple API and other software and related Ripple Documentation, as well as any Updates thereof, delivered pursuant to this Agreement, including any source code provided by Ripple.

1.15 **"Ripple Technology"** means any Technology developed, acquired or licensed by Ripple, including Ripple Developed Technology, Ripple Background Technology and Ripple Derivative Technology (as such terms are defined in Section 5).

1.16 **"Statement of Work"** means a written document detailing certain services and activities of the parties that references this Agreement and that has been mutually agreed upon by the parties.

1.17 **"Support Services"** means support Services for the Integrated Solutions or related Ripple Products that are identified as being the responsibility of Ripple Services in a Statement of Work and that Ripple Services provides to Integrator or, if applicable, a Client.

2

ripple Labs

1.18   "**Technology**" means creations, ideas, inventions, improvements, know-how, concepts, algorithms, protocols, data, processes, procedures, methods, techniques, protocols, formulations, systems, research tools, compositions, code, software, hardware, machines, prototypes, instruments, documents, components, and other materials, information and works of authorship, whether or not patentable, copyrightable, or susceptible to any other form of protection, including any Intellectual Property Rights in such items.

1.19   "**Third Party Claim**" shall mean a claim by any person other than Ripple or Integrator or their Affiliates, including claims by Clients.

1.20   "**Updates**" mean (1) all error corrections, bug fixes, or patches for the Ripple Software and related Ripple Documentation, and (2) all enhancements, modifications, improvements, and upgrades for the Ripple Software and/or related Ripple Documentation that improve the performance of the Ripple Software or that add new functionality or features.

2.   **Development of Integrated Solutions**

2.1   Delivery of Technology. No later than [●] days following the Effective Date, Ripple will provide Integrator with the Ripple Software, Documentation and other Ripple Technology specified in Exhibit A hereto. The Parties will further exchange such Technology as required to permit each Party to perform its obligations under any Statement of Work or as otherwise reasonably requested by a Party.

2.2   Integration Activities. Except as otherwise set forth herein or in a Statement of Work, Integrator will be solely responsible for creating, developing, testing, demonstrating, marketing, distributing and implementing the Integrated Solutions and for providing maintenance, support and other services with respect thereto, all in accordance with the provisions hereof. Ripple will provide Services to support such efforts in accordance with any Statement of Work agreed upon by the Parties in accordance with Section 3 below. Integrator will use commercially reasonable efforts to insure that the Integrated Solutions complies in all material respects with the Ripple Product requirements included in Exhibit A, the Documentation and any Statement of Work, and Ripple shall not be liable for any failure to comply with the foregoing.

2.3   Grant of License by Ripple. Subject to the terms and conditions herein, Ripple hereby grants to Integrator a limited, non-exclusive, non-transferable, right and license during the Term of this Agreement: (a) to access and use the Ripple Software (including related Ripple Documentation and Ripple Technology) to develop and test the Integrated Solutions for use as contemplated herein; (b) to reproduce and distribute the Ripple Software as an integrated part of the Integrated Solutions to Clients as provided in Section 2.4; and (c) to use the Integrated Solutions to access the Ripple Protocol and other Ripple Technology and communicate with the distributed Ripple Network on behalf of itself and its Clients. Integrator shall not make any of the Ripple Documentation available to Clients except as part of Client Documentation for the Integrated Solutions as permitted under Section 2.8.

2.4   Distribution of Ripple Software. In connection with the license granted in Section 2.3, Integrator may: (a) copy, modify and adapt the Ripple Software solely for the purpose of creating the Integrated Solutions, including incorporating, integrating or embedding the Ripple Software with or into the Integrator Software (provided, however, that Integrator shall not reverse engineer the Ripple Software); (b) copy, market and distribute the Ripple Software (including any applicable Ripple Technology) only as part of the Integrated Solutions; and (c) permit Clients to use, or to benefit from Integrator's use of, the Ripple Software (and applicable Ripple Technology) as

3

rippleLabs

part of the Integrated Solutions to access the Ripple Protocol and other Ripple Products and communicate with the distributed Ripple Network. Integrator may not distribute or sell the Ripple Software or Ripple Technology except as part of the Integrated Solutions (including as a stand-alone application).

    (a)   Integrator will not distribute or make available the Ripple Software or Ripple Technology except to its Clients pursuant to an Client license agreement (a "**Client Agreement**") that includes (i) restrictions on use consistent with the rights granted herein, including prohibitions on distributing, modifying or creating derivative works of any Ripple Software and Ripple Technology; (ii) protections for the Intellectual Property Rights in Ripple Technology under terms no less protective than the protections set forth in this Agreement; (iii) ownership of Ripple Technology consistent with the provisions herein; and (iv) limitations on Ripple's liability relating to use of Ripple Technology on terms substantially similar to those herein; in each case Ripple need not be specifically named if such provisions inure to Ripple's benefit. Integrator shall notify Ripple of each Client with whom it enters into a Client Agreement. Integrator shall promptly notify Ripple if Integrator becomes aware of any breach of any Client Agreement relating to the Integrated Solutions, Ripple Software or Ripple Technology. Upon the termination of any Client Agreement, Integrator will use commercially reasonable efforts to ensure the return or destruction of all copies of the Ripple Software covered by such Client Agreement and all reproductions thereof.

    (b)   Integrator will cause each Client with whom it enters into a Client Agreement to execute and enter into a Ripple End User Agreement in the form attached hereto as Exhibit B. Integrator will promptly provide Ripple with a copy of each such Ripple End User Agreement. Ripple may amend Exhibit B from time to time by giving Integrator written notice and Integrator will use the amended version with Clients on a going forward basis. Ripple will notify Integrator of any breach of a material obligation related to the Ripple Software or Ripple Technology under any Ripple End User Agreement of which Ripple becomes aware.

    2.5   Limitations on License. Except for distribution of the Integrated Solutions as expressly permitted in Section 2.4, the Ripple Software shall only be used for Integrator's own internal business purposes, including support of its Clients. Integrator may copy or duplicate the Ripple Software for normal operational and backup purposes and as is necessary for the performance of its activities hereunder. Integrator, however, will not:

    (a)   modify, translate, decompile, disassemble or reverse engineer any Ripple Technology except as expressly permitted by this Agreement;

    (b)   remove or obscure any proprietary notices (including without limitation any copyright, trademark, service mark, or patent designations), legends, labels, symbols, or logos from any Ripple Technology;

    (c)   sell, assign, lease, rent, loan, distribute, transmit, publish or otherwise transfer or make available any Ripple Technology (with or without charge) to any person, other than in accordance with this Agreement;

4

rippleLabs

(d)   embed, incorporate, merge or combine the Ripple Software into any software, program, application, services, semiconductor chip or other hardware except for the Integrated Solutions as explicitly permitted in this Agreement;

(e)   upload or incorporate any malicious code or otherwise use the Ripple Software or Ripple Products to further any purposes which is illegal or otherwise contrary to the license granted in this Section 2; or

(f)   except as permitted by this Agreement, encumber any Ripple Technology or permit any Ripple Technology to become subject to any lien.

2.6   Reservation of Rights.   All rights with respect to the Ripple Products, Ripple Software and Ripple Technology not specifically granted to Integrator hereunder are reserved by Ripple, and Ripple Labs remains the owner of all right, title, copyright and interest in the Ripple Software and any copies of it. Integrator acknowledges that its and its Clients' use of the Ripple Protocol, Ripple Network and other Ripple Products shall be subject to all applicable terms and conditions established for such items from time to time.

2.7   No Exclusivity. Subject to a Party's confidentiality obligations under Section 8 and to the other Party's Intellectual Property Rights, each Party reserves the right to (a) market, promote, license and sublicense, sell, distribute, otherwise dispose of, maintain, support, service, and otherwise commercialize its products and services either directly to end users or indirectly through other sales representatives, systems integrators, resellers, or other third parties, (b) develop and implement interfaces with other third parties, (c) discontinue the development, manufacture, license, sale, distribution, other disposition, maintenance, support, service, or other commercialization of its software, products and services, and (d) improve or change the design or functionality of its software, products and services.

2.8   Creation of Client Documentation.   Integrator may incorporate reasonable and necessary information from the Ripple Documentation into end user documentation for the Integrated Solutions that is to be provided to Clients ("**Client Documentation**"); provided that Integrator will not incorporate any Ripple Confidential Information or other non-public information concerning the Ripple Software or Ripple Products without the prior written consent of Ripple which may be withheld in Ripple's sole discretion.   Integrator may not use the Client Documentation other than in connection with the Integrated Solutions and Ripple Products or distribute it to any third parties other than Clients.

2.9   Grant of License by Integrator. Subject to the terms and conditions herein, Integrator hereby grants to Ripple a limited, non-exclusive, non-transferable, royalty free right and license during the Term of this Agreement: (a) to access and use the Integrator Software (including related Documentation) made available by Integrator to perform Services, and (b) to develop and test the Integrated Solutions for use as contemplated herein. Integrator represents and warrants to Ripple that as of the Effective Date and continuing through the Term that it has the right and authority to grant the foregoing license.

2.10   Certification. If specified in a Statement of Work, the Integrated Solutions will be certified prior to being connected to the Ripple Protocol production environment and prior to making the Integrated Solutions available to any third party for production use. In order for the Integrated Solutions to be certified, it must perform in all material respects in accordance with Ripple's internal testing requirements as mutually agreed by the Parties as set forth in a mutually agreed Statement of Work (**"Conformance Testing"**). Integrator shall make the Integrated

5

rippleLabs

Solutions available for Conformance Testing by a mutually agreed, commercially reasonable method, provided that, in all cases the Integrator shall have the right to control Ripple's access to the Integrated Solutions during any such Conformance Testing and that nothing in this provision shall require Integrator to reveal any information or materials, the revelation of which would cause Integrator to forfeit the protection of any Intellectual Property Rights or breach an obligation of confidentiality to any party with respect to such information or materials. The Services of Ripple in performing the Conformance Testing, if any, including any applicable charges, will be detailed in a Statement of Work. Upon the completion of the Conformance Testing and no later than five (5) days after the end of the relevant testing period as defined in the applicable Statement of Work, Ripple will notify Integrator in writing of any non-conformities or defects found. Once all identified non-conformities or defects have been corrected the Integrated Solutions will be resubmitted for additional Conformance Testing, and the process of testing, notification and correction will repeat until all non-conformities and defects have been corrected or eliminated as evidenced by written acknowledgment signed by Ripple.

2.11 Procurement. Unless otherwise agreed to in writing by the Parties, Integrator or its Clients will be solely responsible for obtaining all hardware and the operating software for such hardware necessary to use the Integrated Solutions and Ripple Products and for paying all fees in connection therewith. In no event will Ripple have any responsibility, liability or obligation with respect to any such hardware, software or any problems experienced by Integrator or Clients relating to the use of such hardware or software, including, but not limited to, any non-conformance of such hardware or software with the information available to developers of applications for operation on such hardware and software, or any viruses, bugs or other errors that may be resident in such software.

2.12 Implementation. Except as expressly agreed in a Statement of Work, Integrator will be responsible for conducting all activities required to enable access to the Integrated Solutions and Ripple Products at its Client's locations and for providing training to such Clients. All such installation and training will be conducted in accordance with generally accepted industry standards and Integrator's best practices.

2.13 Marketing Efforts and Technical Capability. Integrator will maintain a staff of capable sales and technical personnel who have adequate ability to: (a) introduce, promote and market the Integrated Solutions; (b) provide accurate information to Clients concerning the features and capabilities of the Integrated Solutions and related Ripple Products; and (c) provide post-distribution technical assistance and support and maintenance to Clients in connection with the Integrated Solutions and its interaction with Ripple Products as provided herein.

2.14 Distribution. Except as expressly agreed in a Statement of Work, Integrator will only distribute, license, and make the Integrated Solutions available to its Clients directly and will not permit, directly or indirectly, any third party to distribute, sell, resell or make the Integrated Solutions available to any Client.

2.15 Approvals. Integrator will obtain, at its own expense, all registrations, licenses and approvals from all authorities and agencies which may be needed in order for Integrator to exercise its rights and perform its obligations under this Agreement and to enable use of the Integrated Solutions and Ripple Products by its Clients.

2.16 Updates. Ripple will make Updates available to Integrator (including through Ripple Services) in Ripple's sole discretion. Any Update provided to Integrator or Clients will be included in the term "Ripple Software." If Ripple provides an Update to Integrator which is identified as

6

rippleLabs

being intended to correct errors, increase performance or mitigate risk and/or the legal liability of either Party. Integrator shall use reasonable efforts to insure that the Integrated Solutions are modified to use such Updates and that its Clients receive the benefits of the Update. Integrator agrees to use commercially reasonable efforts to make necessary changes to the Integrated Solutions to accommodate Upgrades and new versions of the Ripple Products within three (3) months of Ripple providing the final specifications of such Upgrades and new versions to Integrator. Ripple will provide development support reasonably required by Integrator to facilitate such changes to the Integrated Solutions. Ripple will use its commercially reasonable efforts to notify Integrator in advance of informing mutual Clients of Upgrades and new versions of Ripple Products where such changes may cause a material impact to the Integrated Solutions or use thereof.

     2.17   Use of Competing Technologies. During the Term, Integrator agrees that it will not, directly or indirectly (including through its Affiliates), without the written permission of Ripple: (i) fork any part of the Ripple Software; (ii) replace the Ripple Technology used in or with the Integrated Solution with any competing or alternative technology; (iii) engage in any Competing Activities or work with, control or participate in the business of any individual, firm, corporation, institution or company engaged in Competing Activities. **"Competing Activities"** means to design, specify, support, develop, integrate, market, promote, license, sell, distribute, or otherwise commercialize in any manner any product or protocol which is competitive with or a substitute for the Ripple Software or Ripple Protocol.

3.   **Services**

     3.1   Statements of Work. Integrator may request that Ripple provide consulting or other Services to Integrator or Clients, including Integrated Solutions development services, certification Services and technical support Services. Ripple Services will use commercially reasonable efforts to render the Services as set forth in each Statement of Work between Ripple and Integrator (collectively, **"Services"**), and deliver any deliverables which may be specified therein. Ripple shall have no obligation to perform Services until and unless it accepts a Statement of Work in writing. The Statement of Work will be in a form to be agreed between the Parties and will set forth the type and scope of work to be performed, project timeline and milestones, acceptance criteria and fees owed for the Services. Any such Statement of Work will reference, form a part of, and be governed by the terms of this Agreement. Integrator shall reimburse Ripple for expenses incurred in connection with the Services as specified in the Statement of Work. Unless otherwise specified in a Statement of Work, Services are provided on a time and materials basis, and any budgets or estimated hours or costs in a Statement of Work are non-binding estimates only. Ripple will notify Integrator as soon as it becomes aware that an estimate will be exceeded and agrees not to exceed estimated fees absent written and signed approval (but shall not be required to continue to provide Services until additional fees are approved). In the event of a conflict between the terms of a Statement of Work and this Agreement, the terms of this Agreement will control, unless the Statement of Work explicitly specifies that the conflicting provision will control.

     3.2   Support and Maintenance Services.

     (a)   Technical Support Services. Ripple will provide Integrator with Support Services, including software maintenance service and technical support services, for the Ripple Software and Ripple Products as set forth in a Statement of Work in exchange for the Fees specified therein. Except as otherwise set forth in a Statement of Work, Ripple will not be required to provide on-site Support Services.

7

     RPLI_SEC 0095219

rippleLabs

(b) Client Support Services. Ripple will provide Integrator with telephonic, email and remote assistance in supporting Clients and the Integrated Solutions (e.g., Level 2 Support) as further detailed in a Statement of Work. Unless otherwise set forth in a Statement of Work, as between the Parties, Integrator will be solely responsible for providing Clients with maintenance and support of the Integrated Solutions (and related Ripple Products) and Integrator Products (e.g., Level 1 Support), as well as with related training, installation and other technical and professional services. Upon mutual agreement of the Parties in a Statement of Work, Integrator may subcontract with Ripple for the performance of certain of these Support Services. For each Client to whom Ripple provides Support Services, Integrator will pay Ripple the Fees set forth in the Statement of Work. Notwithstanding any provision of this subsection, in the event a Client contacts Ripple directly regarding first-line support of the Ripple Software or Ripple Products, Ripple may respond directly to the Client or refer the Client to Integrator, but in any case will inform Integrator of the nature of Client's request, Ripple's recommendations, the actions taken, and results.

(c) Pre-Releases. Ripple will notify Integrator of pre-release alpha or beta versions of Updates to the Ripple Software. Upon Integrator's request, Ripple will make such pre-releases reasonably available to Integrator, at no additional cost, for review, evaluation, training, and planning purposes. Ripple will make good faith efforts to make each such pre-release available to Integrator no later than the earliest date Ripple makes such pre-releases available to any other client. All such pre-releases are provided "**AS IS**," without warranty of any kind.

3.3   **Training Services.** Unless otherwise set forth in a Statement of Work, as between the Parties, Integrator will be solely responsible to provide training, services to Clients. Ripple will provide training for the Ripple Software to Integrator's implementation staff and technical support personnel as provided in a Statement of Work.

3.4   Implementation Services. Unless otherwise set forth in a Statement of Work, as between the Parties, Integrator will be solely responsible to provide installation and other technical and professional services to Clients. Upon mutual agreement of the Parties in a Statement of Work, Ripple will provide on-site implementation assistance to Integrator staff and technical support personnel for Client implementations of the Integrated Solutions. Integrator will pay Ripple a percentage of the implementation fees received by Integrator for such Services as agreed in a Statement of Work.

3.5   Cooperation. Integrator will provide, in a timely and professional manner and at no cost to Ripple, full assistance and cooperation as may be reasonably requested by Ripple Services to enable the Services to be performed, including the provision of information and data which is complete and accurate; the provision of sufficient access to any equipment, computers, networks (including, VPN access), programs, files, documentation, test data, and sample outputs; and the provision of a suitable work environment when on-site. Ripple Services will not be liable for any deficiency in performing the Services if such deficiency results from Integrator's or a Client's failure to provide such cooperation. Ripple Services' representatives will comply with reasonable written rules and regulations of Integrator or a Client with respect to on-site work, provided that such rules and regulations are provided to Ripple Services prior to commencement of the Services.

3.6   Service Remedies. Services and deliverables will be considered accepted upon delivery unless the Statement of Work sets forth an alternative acceptance process. In the event

8

RPLI_SEC 0095220

rippleLabs

that Ripple Services fails to provide any portion of the Services, Ripple Services will, at its sole option and expense, re-perform that portion of the Services or refund the fees paid, if any, for that portion of the Services; provided, however, that Ripple Services will be excused from its performance of the Services to the extent that any Technology, data, information, materials or assistance provided, directly or indirectly, by or on behalf of Integrator to Ripple Services to enable Ripple Services to perform the Services contains errors or defects, cannot be used to perform the Services or is insufficient or unsuited to enable Ripple Services to perform the Services. THE FOREGOING REMEDY WILL CONSTITUTE RIPPLE'S ENTIRE LIABILITY, AND INTEGRATOR'S SOLE AND EXCLUSIVE REMEDY, WITH RESPECT TO RIPPLE'S FAILURE TO PERFORM THE SERVICES. For clarification, in no event will Ripple Labs be required to perform any Services for Integrator, any Client or any other entity under or in connection with this Agreement or any Statement of Work.

4.   **Sales and Marketing**

4.1   Press Release and Marketing Announcement.   Following execution of this Agreement, the Parties will issue a mutually agreed joint press release announcing the Parties' relationship. A Party may place marketing content obtained from or approved by the other Party on its corporate web site and other marketing materials, including a description of the Parties' arrangement hereunder. Each Party must obtain prior written approval from the other Party for all written materials that purport to represent the other Party and its products and services.

4.2   Marketing Plan. Ripple and Integrator agree to use good faith efforts to discuss whether to pursue joint sales and marketing activities. Any joint sales and marketing activities, which are planned to be undertaken by the Parties will be set forth in a Statement of Work to this Agreement (a **"Marketing Plan"**). The Marketing Plan will set forth the joint business and marketing strategies and general obligations with respect to the Parties' relationship and the promotion of the Integrated Solutions and the related Products and services of the Parties, including marketing materials, appropriate wording, advertisement strategies, budget, office and staff requirements.

   (a)   The Parties may decide in the Marketing Plan to jointly develop marketing materials for the Integrated Solutions and applicable Products of the Parties. In furtherance of developing these Materials and upon request, each Party shall provide the other with any and all existing marketing materials for its applicable Products and Software.

   (b)   In pursuing joint sales and marketing activities, each Party's personnel shall at all times conduct themselves in a manner and means that reflects favorably upon the other Party. Furthermore, in any Marketing Plan, each Party will designate an individual from their organization who will be accessible and responsive to the other Party and assist the sales staff of the other Party in properly marketing the other Party's Products and services, in preparing responses to RFPs and coordinating prospects between the two Parties (the **"Channel Managers"**). The Channel Managers shall communicate with one another to jointly plan integration activities, respond to RFPs, coordinate prospect lists and plan joint marketing activities.

   (c)   Ripple and Integrator agree to meet at least semi-annually or on another mutually agreed schedule and upon either Party's request with no less than twenty (20) days' notice at a mutually convenient time and location (or via teleconference), in order to further discuss the Marketing Plan and their joint sales and marketing activities and

9

rippleLabs

joint business objectives. Failure to adhere to the terms of this Section shall not constitute a breach of this Section by either Party unless a Party unreasonably refuses to meet.

(d)   Subject to other provisions of this Agreement, each Party shall bear the cost of the marketing and sales expenses specific to each Party.

4.3   Integrated Solutions Promotion. Upon successful launch of the Integrated Solutions and the award of Certification if required hereunder, each Party may provide a mutually agreed description of the Integrated Solutions and the Parties' relationship on its corporate web site and in other marketing materials deemed appropriate by both Parties, including but not limited to establishing links from a page on each Party's website to a page on the other Party's website. The content, format and placement of such links will be as mutually agreed to by the Parties.

4.4   Trademark Approval. All uses by a Party of the other Party's trademark, logo or trade name (a "**Trademark**") in any advertisement, publication, web page, press release, marketing materials or other manner ("**Materials**") shall be submitted to the Party owning such Trademark (the "**Brand Owner**") for written approval prior to such use, distribution, display or publication thereof. The Brand Owner shall notify the other Party, as applicable, in writing whether it approves of such Materials, such approval not to be unreasonably withheld. In the event that a Brand Owner disapproves of any use or Material, the other Party shall promptly incorporate any corrections or revisions required by the Brand Owner or remove reference to the Brand Owner's Trademark before using such Material. Subject to the terms and conditions of this Agreement, a Brand Owner hereby grants to the other Party a non-exclusive, royalty-free license to use the Brand Owner's Marks during the Term of this Agreement, solely in connection with the activities contemplated by this Agreement. The license granted in this Section is personal to the receiving Party and is not transferable or sublicensable by such Party (except to permit a vendor to create tangible Materials authorized hereunder for the benefit of a Party). A Party's use of the Brand Owner's trademarks shall comply with the Brand Owner's trademark guidelines (as may be provided by the Brand Owner from time to time) and all legal requirements applicable to such use. All use of a Brand Owner's trademarks, and all good will arising out of such use, will inure to the sole benefit of the Brand Owner. A Party shall clearly indicate a Brand Owner's ownership of any such trademarks and trade names and other proprietary marks. Each Party recognizes the validity of the title to and ownership of the Trademarks by the Brand Owner and will not take any action, either directly or indirectly, that may in any way impair the validity of or the Brand Owner's ownership of its Trademarks. A Party will not during the Term of this Agreement or at any time thereafter, use or register (with any governmental or other authority, local or foreign) any trademark or trade name identical with, or confusingly similar to, any of another Party's Trademarks without the prior written consent of the Brand Owner.

4.5   No Endorsement. A Brand Owner's Trademarks shall not be used in any manner to suggest or imply an endorsement by the Brand Owner of any product or service available from the other Party, online or otherwise, unless the Brand Owner expressly agrees in writing to the terms of the endorsement or other approval and to the use of the Trademarks in connection with that endorsement or approval. The foregoing shall not prevent the Parties from accurately disclosing the existence of the Integrated Solutions, the relationship between the Parties, and/or representing that the Integrated Solutions has been Certified hereunder. A Brand Owner's Trademarks shall not be used to imply any relationship between the parties other than that explicitly set forth in this Agreement. If requested by a Brand Owner, the other Party agrees to publish any affiliation disclaimer requested by the Brand Owner in a conspicuous manner and in a prominent location, including on Materials.

10

RPLI_SEC 0095222

rippleLabs

5.   **Ownership of Technology and Intellectual Property.**

       5.1   Definitions.

       (a)   **"Integrator Background Technology"** means all Technology that Integrator or any of its Affiliates or Clients (i) has developed, acquired or licensed prior to the Effective Date, or (ii) develops, acquires or licenses entirely independently of its activities under this Agreement and without any reference to any information, data, materials, Ripple Technology or Ripple Confidential Information. Notwithstanding anything to the contrary herein, all Integrator Derivative Technology will be deemed to be Integrator Background Technology.

       (b)   **"Integrator Derivative Technology"** means any Technology (including works of authorship, materials, software, HTML, writings, drawings, designs, and specifications in which such Technology is embodied) that is conceived, created or otherwise developed by or for either Party or a Client (alone or with others) and that is a Derivative of the Integrator Background Technology. Integrator Derivative Technology does not include improvements, modifications, customizations or derivatives of the Ripple Background Technology or any Ripple Derivative Technology.

       (c)   **"Integrator Developed Technology"** means all Technology that Integrator or any of its Affiliates, Representatives or Clients conceives, creates or otherwise develops during the performance of any activities relating to the Integrated Solutions under this Agreement, but excluding any Ripple Background Technology and Integrator Background Technology.

       (d)   **"Ripple Background Technology"** means all Technology that Ripple or any of its Affiliates (i) has developed, acquired or licensed prior to the Effective Date, or (ii) develops, acquires or licenses entirely independently of its activities under this Agreement and without any reference to any information, data, materials, Integrator Technology or Integrator Confidential Information. Notwithstanding anything to the contrary herein, (1) all Ripple Derivative Technology will be deemed to be Ripple Background Technology, and (2) for the avoidance of doubt, Ripple Background Technology will be deemed to, and will, include the Ripple Software.

       (e)   **"Ripple Derivative Technology"** means (i) any Technology (including works of authorship, materials, software, HTML, writings, drawings, designs, and specifications in which such Technology is embodied) that is conceived, created or otherwise developed by or for either Party or a Client (alone or with others) and that is a Derivative of the Ripple Background Technology (including the Ripple Software); and (ii) any suggestions or proposals regarding new or improved features, functionality or performance of the Ripple Software or Ripple Products. For example, as defined in this Agreement, the data output of Ripple Software when employed by Integrator or third party software program would *not* transform that software program into "Ripple Derivative Technology" merely because it employs the output of the Ripple Software as permitted under this Agreement. Likewise, the software code utilized to link the Integrator Software and Ripple Software will not serve to constitute Ripple Derivative Technology if it does not contain any portion of Ripple Software.

11

rippleLabs

(f)   **"Ripple Developed Technology"** means all Technology that Ripple or any of its Affiliates or Representatives conceives, creates or otherwise develops during the performance of any activities relating to the Integrated Solutions under this Agreement, but excluding any Ripple Background Technology and Integrator Background Technology.

5.2   Background Technology. As between the Parties, Integrator will own and retain ownership of all right, title, and interest in and to all Integrator Background Technology. Ripple does not acquire any rights, express or implied, in any Integrator Background Technology, other than those expressly specified in this Agreement. As between the Parties, Ripple Labs will own and retain ownership of all right, title, and interest in and to all Ripple Background Technology. Integrator does not acquire any rights, express or implied, in any Ripple Background Technology, other than those expressly specified in this Agreement.

5.3   Developed Technology. As between the Parties, Integrator will own and retain ownership of all right, title, and interest in and to all Integrator Developed Technology. Ripple does not acquire any rights, express or implied, in any Integrator Developed Technology, other than those expressly specified in this Agreement. As between the Parties, Ripple Labs will own and retain ownership of all right, title, and interest in and to all Ripple Developed Technology. Integrator does not acquire any rights, express or implied, in any Ripple Developed Technology, other than those expressly specified in this Agreement.

5.4   Derivative Technology. Integrator agrees to disclose promptly in writing and deliver to Ripple Labs all Ripple Derivative Technology that it conceives, creates or develops. All Ripple Derivative Technology will be considered Ripple Background Technology and the sole and exclusive property and Confidential Information of Ripple Labs. Except as set forth in this Agreement, Integrator retains no rights to use the Ripple Derivative Technology and agrees not to challenge the validity of Ripple Labs' ownership in the Ripple Derivative Technology. All Integrator Derivative Technology will be considered Integrator Background Technology and the sole and exclusive property and Confidential Information of Integrator.

5.5   Assignment and Further Assurances. To the extent that a Party retains rights in any Technology, Intellectual Property Rights or other items in contravention of the allocation of ownership set forth in this Section 5, such Party (the **"Assigning Party"**) agrees to and hereby grants, assigns and conveys to the other Party (the **"Owning Party"**) all of the Assigning Party's right, title and interest, if any, in such items and in all patents, copyrights, moral rights and other Intellectual Property Rights associated therewith (**"Conveyed Rights"**).

(a)   To the extent, if any, that any Conveyed Rights are not assignable or the Assigning Party retains any right, title or interest in and to any such items, the Assigning Party (i) unconditionally and irrevocably waives the enforcement of such Conveyed Rights, and all claims and causes of action of any kind against the Owning Party with respect to such Conveyed Rights; (ii) agrees, at the Owning Party's request and expense, to consent to and join in any action to enforce such Conveyed Rights; and (iii) hereby grants to the Owning Party a perpetual, irrevocable, fully paid-up, royalty-free, transferable, sublicensable (through multiple levels of sublicensees), exclusive, worldwide right and license to use, reproduce, distribute, display and perform (whether publicly or otherwise), prepare derivative works of and otherwise modify, make, sell, offer to sell, import, use and exploit (and have others exercise such Conveyed Rights on behalf of the Owning Party) all or any portion of such Conveyed Rights, in any form or media (now known or later developed).

12

rippleLabs

Assigning Party further irrevocably waives any "moral rights" or other rights with respect to attribution of authorship or integrity of such Conveyed Rights that it may have under any applicable law. Assigning Party hereby waives and quitclaims to the Owning Party any and all claims, of any nature whatsoever, which Assigning Party now or may hereafter have for infringement of any Conveyed Rights therein assigned and/or licensed hereunder to the Owning Party.

(b)   Each Party agrees to cooperate fully, both during and after the Term, with the other Party for the purpose of securing, reserving, sustaining, perfecting and protecting a Party's ownership as set forth in this Section 3, including, without limitation, executing such written instruments as may be prepared by Owning Party and doing, at the Owning Party's expense, such other acts as may be necessary in the opinion of Owning Party to obtain a patent, register a copyright, or otherwise enforce Owning Party's rights in such Conveyed Rights (and Assigning Party hereby irrevocably appoints Owning Party and any of its officers and agents as its attorney in fact to act for and on Assigning Party's behalf and instead of Assigning Party, with the same legal force and effect as if executed by Assigning Party).

6.   **Fees and Payment**

6.1   Fees. Integrator will owe Fees to Ripple for the use and/or license of the Ripple Technology and the provision of Services by Ripple as set forth in each Statement of Work (**"Fees"**). All payments made under this Agreement will be in U.S. currency. All Fees are payable within thirty (30) days of the end of each calendar month in which they accrue and will be accompanied by the reports set forth in Section 6.2. Except as otherwise set forth in this Agreement, all fees or other charges will be payable thirty (30) days from the date of invoice. If Integrator fails to pay any outstanding invoice within sixty days of issuance, it will be charged and agrees to pay a late payment fee equal to an annual rate of twelve percent (12%). Such a late payment fee will be calculated on a monthly basis and will be cumulative.

6.2   Reports and Audit. In connection with and at the time of each payment of any Fee, Integrator will submit to Ripple Services a report that contains sufficient information necessary for Ripple Services to determine whether Integrator is paying the correct Fee, including such information as specified in any fee schedule in a Statement of Work and information regarding each Client for whom a Fee is owed. During the Term of this Agreement and for one year thereafter, Ripple may, upon request, audit any and all work, billing or expense records of Integrator relating to actual or potential Fees; provided, however, that such audit shall occur only after reasonable notice to Integrator and shall not unreasonably interfere with Integrator's business or operations.

6.3   Taxes. All federal, state, local, value-added, transfer, sales and use taxes arising out of this Agreement will be paid by the Party required to pay such taxes under applicable law. The Party that is required by applicable law to make the filings, reports or returns and to handle any audits or controversies with respect to any such taxes will do so, and the other Party will cooperate with respect thereto as necessary. All Fees due under this Agreement will be made without any deduction or withholding, unless such deduction or withholding is required by any applicable law of any relevant governmental revenue authority then in effect.

6.4   Integrator's Pricing of Integrated Solutions and Services. Integrator will be free to establish the amounts for all fees it charges to its Clients for the Integrated Solutions and other Integrator Products and to otherwise control the terms and conditions on which it does business with its Clients; provided however that (a) any Client Agreement includes the minimum terms and

13

rippleLabs

conditions as expressed in Section 2.4, and (b) Integrator remains responsible for and pays all Fees and costs for Integrator's and Clients' use of Integrated Solutions as provided hereunder.

7.   **Term and Termination**

7.1   Term. The term of this Agreement ("**Term**") shall continue for a period of three (3) years from the Effective Date, and shall automatically renew for additional one (1) year terms, unless either Party notifies the other, in writing of its decision not to renew at least ninety (90) days prior to the end of the initial term or renewal term.

7.2   Termination for Cause. Either Party shall have the right to terminate this Agreement with immediate effect if the other Party becomes insolvent, or if the other Party materially breaches this Agreement and fails to cure such breach within sixty (60) days or receipt of written notice thereof.

7.3   Termination for Convenience. Each Party may terminate this Agreement without cause by providing at least ninety (90) days' prior written notice to the other Party.

7.4   Effect of Termination.

(a)   A Client may continue using the Ripple Technology as part of the Integrated Solution beyond the termination of this Agreement provided (i) the Client is not in breach of its Client Agreement, (ii) the use is consistent with the terms of this Agreement as if this Agreement were not terminated, (iii) the Client Agreement was entered into prior to the date of termination, (iv) the Client Agreement is not extended by amendment or renewal (over which the Integrator has control) after the termination of this Agreement, and (v) Ripple is provided with any Fees and reports associated with such continued use as if the Agreement were not terminated. If requested by Integrator, Ripple shall continue to provide Support Services pursuant to any Statement of Work existing as of termination in connection with authorized Client use continuing beyond termination, subject to Integrator continuing to provide reports and payments of monies due Ripple for such Support Services, and further provided that Ripple may cease providing such support upon the earlier of (1) such time as the associated Client Agreement expires or terminates, or (2) two (2) years from the date of termination of this Agreement.

(b)   Subject to Section 7.4(a), in the event of a termination or expiration of this Agreement, (a) all licenses and rights granted to the Parties hereunder will terminate, except as expressly set forth herein; (b) all Statements of Work will immediately terminate, and (c) each Party will return or destroy all Confidential Information of the other Party as provided in Section 8.5. Within thirty (30) days after termination or expiration of this Agreement, Integrator shall return any tangible materials and Ripple Technology provided to Integrator by Ripple, except for the Ripple Technology required to support, maintain, or provide related services to then-existing Clients of the Integrated Solutions. Upon termination of this Agreement Integrator agrees to cease marketing, licensing and otherwise making the Integrated Solutions available to new clients or prospective clients.

8.   **Confidentiality And Non-Use**

8.1   Confidential Information. By virtue of this Agreement, a Party may have access to information that is confidential or proprietary ("**Confidential Information**") to the other Party or a

14

ripple Labs

Client. For purposes of this Agreement, "Confidential Information" of a Party means Technology, information, ideas, materials or other subject matter of such Party (including with respect to Integrator, its Clients), whether disclosed orally, in writing or otherwise, that is provided under circumstances reasonably indicating that it is confidential or proprietary. Confidential Information includes, but is not limited to, all business plans, strategies and pricing data; methodologies, algorithms, protocols and analytical routines; software code, APIs and technical information; customer and supplier lists; Intellectual Property Rights; and financial information or materials; in each case, disclosed or otherwise provided by one Party (the **"Disclosing Party"**) to the other Party (the **"Receiving Party"**). Without limitation to the foregoing, (i) all Integrator Software and Integrator Technology will be deemed to be Confidential Information of Integrator, (ii) all Ripple Software and Ripple Technology will be deemed to be Confidential Information of Ripple Labs, and (iii) Confidential Information under this Agreement shall not include transaction or other information transmitted through the Ripple Protocol or via the Ripple Network. Ripple acknowledges that it may have access to confidential or proprietary information of Clients in connection with this Agreement and that all such information shall be deemed the Confidential Information of Integrator protected under this Section 8.

8.2   Restrictions on Use. A Receiving Party shall not use Confidential Information of the Disclosing Party for any purpose other than in furtherance of this Agreement and the activities described herein. Integrator is expressly prohibited from using or allowing or disclosing to any third parties to use, any of the Confidential Information of Ripple in any way to design, develop, market, promote, distribute, or otherwise exploit any products or services owned or developed by Integrator or any third party which compete with the Integrated Solutions, the Ripple Products or any portion thereof. The Receiving Party shall not disclose Confidential Information of the Disclosing Party to any third parties other than those Affiliates, employees, advisors, contractors, agents or Clients who have a legitimate need to know such Confidential Information ("**Representatives**"). Each Party agrees that its Representatives shall be bound to retain the confidentiality of Confidential Information under provisions (including provisions relating to nonuse and nondisclosure) no less restrictive than those required for Confidential Information hereunder (in the case of Representatives that are not employees of the Receiving Party such agreement shall be in a writing signed by such Representatives). A Receiving Party shall be responsible for any misuse or disclosure of Confidential Information, or any other breach of this Agreement, by any of its Representatives as if Receiving Party had effected such act or omission itself. A Receiving Party shall protect Confidential Information of the Disclosing Party using reasonable care and commercially reasonable information safeguards. A Receiving Party shall advise the Disclosing Party in writing of any misappropriation or misuse of Confidential Information of the Disclosing Party of which the Receiving Party becomes aware.

8.3   Exclusions. This Agreement imposes no obligation upon a Receiving Party with respect to the Confidential Information that the Receiving Party can show: (a) was already in the Receiving Party's possession at the time it was acquired from the Disclosing Party; (b) is or becomes publically available other than as a result of any action or inaction of the Receiving Party or its Representatives; (c) is lawfully obtained by the Receiving Party from a third party without a duty of confidentiality; or (d) is independently developed by the Receiving Party without use of or reference to the Disclosing Party's Confidential Information. In addition, this Section 8 shall not prevent the Receiving Party from disclosing Confidential Information of the Disclosing Party to the extent required by a judicial order or other legal obligation, provided that, in such event, the Receiving Party shall promptly notify the Disclosing Party to allow intervention (and shall cooperate with the Disclosing Party) to contest or minimize the scope of the disclosure (including application for a protective order).

15

＊ripple Labs

8.4   Terms of This Agreement. Notwithstanding anything to the contrary in this Agreement, except to the extent otherwise required by law, neither Party will disclose the terms of this Agreement to any third party without the express prior written consent of the other Party; provided, however, that either Party may disclose the terms of this Agreement to its attorneys and accountants or any potential investor or acquirer of a substantial part of such Party's business or assets, whether by merger, sale of assets, sale of stock or otherwise, or as otherwise may be required by law.

8.5   Return of Confidential Information. Upon termination of this Agreement, each Party (as Receiving Party) will immediately return to the Disclosing Party all Confidential Information of the Disclosing Party embodied in tangible (including electronic) form or, at the Disclosing Party's discretion, destroy all such Confidential Information and certify in writing to the Disclosing Party that all such Confidential Information has been destroyed; provided that electronic data shall be subject to a Party's normal backup destruction policies.

8.6   Survival. Any provisions of this Agreement, which are intended by their specific terms or by necessary implication, to survive the expiration or termination of this Agreement will so survive. Without limitation to the generality of the foregoing, Sections 5, 6.2, 7.4, 8, 9.2, 10, 11 and 13 will survive the termination or expiration of this Agreement.

9.   **Warranties**

9.1   Representations and Warranties. Each Party represents and warrants to the other Party that as of the Effective Date and continuing through the Term: (i) it is not precluded by any existing arrangement, contractual or otherwise, from entering into this Agreement and performing hereunder; and (ii) it has the full right, power and authority to enter into this Agreement and to carry out its obligations hereunder and grant the rights granted by it hereunder, and there are no impediments known to it which would prevent its compliance with all the terms of this Agreement.

9.2   Disclaimers. THE RIPPLE SOFTWARE AND RIPPLE PRODUCTS AND ANY OTHER MATERIALS, INFORMATION AND SERVICES PROVIDED BY RIPPLE TO INTEGRATOR AND CLIENTS ARE PROVIDED "AS IS." TO THE MAXIMUM EXTENT PERMISSIBLE BY LAW, RIPPLE PROVIDES NO, AND HEREBY EXPRESSLY DISCLAIMS, ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE, ACCURACY AND NON-INFRINGEMENT, AND ALL WARRANTIES THAT MAY ARISE OUT OF COURSE OF DEALING, COURSE OF PERFORMANCE OR USAGE OF TRADE IN CONNECTION WITH THE SERVICES, RIPPLE SOFTWARE, RIPPLE PRODUCTS OR OTHERWISE. IT IS THE RESPONSIBILITY OF INTEGRATOR TO EVALUATE THE ACCURACY, COMPLETENESS AND USEFULNESS OF ALL DATA AND RESULTS GENERATED THROUGH ITS RECEIPT OF THE SERVICES, RIPPLE SOFTWARE OR RIPPLE PRODUCTS OR USE THEREOF.

10.   **Indemnification**

10.1   Ripple Indemnification.

(a)   Ripple Services will indemnify, defend and hold Integrator and its Affiliates and each of their employees, officers, directors and agents harmless from and against any and all Losses suffered, incurred or sustained by any of them, or to which any of them become subject, as a result of any Third Party Claim arising from or in connection with: (i) the marketing, promotional and/or advertising activities of Ripple and its Representatives in connection with the Ripple Software or Ripple Products; (ii) unauthorized representations or warranties made by Ripple or its Representatives

16

ripple Labs

regarding the Integrator Software or Integrator Products, including the Integrated Solutions; (iii) any failure by Ripple or its Affiliates to comply with applicable laws; (iv) any breach by Ripple or its Representatives of any warranty or obligation of this Agreement; or (v) any claim of personal injury or tangible property damage caused by any gross negligence or willful misconduct of Ripple or its Representatives during the provision of the Services.

(b)   Ripple Services will have no liability for any Third Party Claim to the extent that any Third Party Claim is based upon or attributable to: (1) any act, neglect, default or liability of Integrator or its Affiliates or their directors, officers, managers, employees, agents, consultants or Representatives; (2) misuse, abuse or neglect of the Ripple Software, Ripple Products or Services by any party other than Ripple; (3) use of other than the then-current, unaltered version and release of the applicable Ripple Software, Ripple Products or Services; (4) use, modification, operation or combination of the Ripple Software, Ripple Products or Services with any other products or services not provided or approved by Ripple; (5) Integrator's failure to fully comply with this Agreement, the Documentation and any other reasonable instructions of Ripple; (6) any data, information, materials Technology or Intellectual Property Rights provided, directly or indirectly, by or on behalf of Integrator to Ripple; (7) any problems or issues with any third party hardware, software, telecommunications systems or any other materials (including, without limitation, third party software contained in or provided along with the Ripple Software, Ripple Products or Services); or (8) any actions or omissions of a Client or any third party participant in the Ripple Network.

10.2   Integrator Indemnification.

(a)   Integrator will indemnify, defend and hold Ripple and its Affiliates and each of their employees, officers, directors and agents harmless from and against any and all Losses suffered, incurred or sustained by any of them, or to which any of them become subject, as a result of any Third Party Claim arising from or in connection with: (i) the marketing, promotional and/or advertising activities of Integrator and its Representatives in connection with the Integrated Solutions, Integrator Software or Integrator Products; (ii) unauthorized representations or warranties made by Integrator or its Representatives regarding the Ripple Software or Ripple Products; (iii) any failure by Integrator or its Affiliates to comply with applicable laws; (iv) any allegations that the Integrator Software or Integrator Products, including the Integrated Solutions (excluding any part of the Ripple Software incorporated therein) or any Integrator Technology, infringes or misappropriates a third party's intellectual property or other proprietary rights; (v) any unauthorized use, misuse, abuse or neglect of the Ripple Software or the Ripple Products by Integrator or its Representatives; (vi) any breach by Integrator or its Representatives of any warranty or obligation of this Agreement; (vii) any claim brought by any Client, including any claim regarding the use or inability to use the Integrated Solutions or any Ripple Products or Ripple Technology, other than any Third Party Claim resulting from a breach of this Agreement by Ripple; and (viii) any claim of personal injury or tangible property damage caused by any gross negligence or willful misconduct of Integrator or its Representatives.

(b)   Integrator will have no liability for any Third Party Claim to the extent that any Third Party Claim is based upon or attributable to any act, neglect, default or liability of Ripple, its directors, officers, managers, employees, agents, consultants or

17

RPLI_SEC 0095229

rippleLabs

Representatives, including without limitation any modification or use of the Integrated Solutions by Ripple in a manner that Integrator did not authorize or any use by Ripple of the Integrated Solutions in combination with a product or service that Integrator did not recommend or approve.

10.3   Indemnification Procedure.   A person asserting indemnification rights against a Party with respect to a Third Party Claim must: (a) give such Party prompt written notice of such Third Party Claim (provided that any delay in such notice will not relieve the indemnifying Party from its obligations to the extent it is not prejudiced thereby); (b) permit such Party to control the defence of such Third Party Claim and the negotiation of any settlement, provided, however, that the indemnifying Party may not agree to settle any Third Party Claim in a manner that adversely affects the indemnified Party without the consent of the indemnified Party; and (c) cooperate with such Party in such defense and negotiation at the indemnifying Party's expense. The indemnification rights of the Parties under this Section are their sole and exclusive remedies with respect to any Third Party Claims described herein.

11.   Limitation of Liability and Damages

11.1   NEITHER PARTY GUARANTEES THAT ACCESS TO ITS SOFTWARE OR PRODUCTS, OR INFORMATION AVAILABLE THROUGH ITS PRODUCTS, WILL BE UNINTERRUPTED, THAT SUCH ITEMS WILL BE FREE OF VIRUSES OR OTHER HARMFUL COMPONENTS OR THAT SUCH ITEMS CANNOT BE HACKED, TAMPERED WITH OR MALICIOUSLY ACCESSED BY THIRD-PARTIES.

11.2   NEITHER PARTY WILL BE LIABLE FOR ANY INDIRECT, EXEMPLARY, SPECIAL, CONSEQUENTIAL OR INCIDENTAL DAMAGES OF ANY KIND (INCLUDING, WITHOUT LIMITATION, LOST PROFITS AND DAMAGES FOR LOST DATA, LOST TRANSACTIONS, LOST ACCOUNTS AND WORK DELAYS), EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

11.3   TO THE MAXIMUM EXTENT PERMISSIBLE BY LAW AND NOTWITHSTANDING ANYTHING IN THIS AGREEMENT TO THE CONTRARY OR ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY OR LIMITATION OF LIABILITY, RIPPLE'S AGGREGATE LIABILITY IN CONNECTION WITH THIS AGREEMENT, THE RIPPLE SOFTWARE, RIPPLE PRODUCTS OR THE SERVICES, REGARDLESS OF THE FORM OF ACTION GIVING RISE TO SUCH LIABILITY (WHETHER IN CONTRACT, TORT OR OTHERWISE) WILL NOT EXCEED THE AGGREGATE FEES ACTUALLY PAID BY INTEGRATOR TO RIPPLE UNDER THIS AGREEMENT IN THE 12 MONTHS PRECEDING THE ACT OR OMISSION GIVING RISE TO THE CLAIM.

11.4   NOTWITHSTANDING ANYTHING TO THE CONTRARY, THE LIMITATIONS IN SECTIONS 11.2 AND 11.3 WILL NOT APPLY WITH RESPECT TO BREACH OF A PARTY'S CONFIDENTIALITY OBLIGATIONS HEREUNDER, INFRINGEMENT OF THE OTHER PARTY'S INTELLECTUAL PROPERTY RIGHTS, OR WITH RESPECT TO DAMAGES FOR WHICH A PARTY HAS AN OBLIGATION TO INDEMNIFY THE OTHER PARTY HEREUNDER. IN NO EVENT SHALL A PARTY HAVE LIABILITY OF ANY NATURE FOR CLAIMS TO THE EXTENT ARISING OUT OF ACTS OR OMISSIONS OF THE OTHER PARTY, ITS AFFILIATES, EMPLOYEES OR REPRESENTATIVES IN BREACH OF THIS AGREEMENT. THE LIMITATIONS OF LIABILITY CONTAINED IN THIS AGREEMENT ARE A FUNDAMENTAL PART OF THE BASIS OF EACH PARTY'S BARGAIN HEREUNDER, AND NEITHER PARTY WOULD ENTER INTO THIS AGREEMENT ABSENT SUCH LIMITATIONS.

18

RPLI_SEC 0095230

rippleLabs

12. Insurance

12.1   Each Party will maintain at its own expense the following insurance:

(a)   **Workers' Compensation Insurance** including Occupational Disease and Employer's Liability in accordance with statutory limits with respect to all employees and agents entering upon the property of the other Party or its customers;

(b)   **General Liability Insurance** with a combined single limit of $2,000,000 per accident and $2,000,000 aggregate for bodily injury and property damage liability; and

(c)   **Products/Completed Operations Liability** (found under general liability) or **Errors and Omissions Professional Liability** with an aggregate limit of $2,000,000 covering liabilities arising out of products and services provided under this Agreement.

12.2   Each Party shall provide the other Party with a certificate of insurance evidencing such coverage and will name the other Party as an additional insured as its interests may appear within (15) days of signing this Agreement.

13. Miscellaneous

13.1   Compliance with Applicable Laws.   Both Parties shall comply with all applicable laws, rules in regulations in the performance of their obligations under this Agreement, including but not limited to the USA Patriot Act. Each Party agrees that it will not offer or agree to offer a government official, political party or candidate for governmental office anything of value to obtain or retain business, and that it will comply with the U.S. Foreign Corrupt Practices Act and the regulations issued thereunder. In addition, the Parties agree to comply with the sanctions laws, rules and regulations administered by the U.S. Department of Treasury's Office of Foreign Assets Control. Furthermore, neither Party shall utilize the other Party's Products in a manner that could cause the other Party to violate any applicable laws, rules or regulations to which it is subject.

13.2   Force Majeure. Except with respect to Integrator's obligation to make timely payments, neither Party will be responsible for any delay or failure in performance to the extent that such delay or failure is caused by fires, strikes, embargoes, explosion, earthquakes, floods, wars, labor disputes, government requirements, civil or military authorities, acts of terrorism, acts of God or other causes beyond its reasonable control. In the event of such a Force Majeure condition extending for more than one hundred and thirty (30) days, the affected Party shall have the right, but not the obligation, to terminate this Agreement.

13.3   Severability. If any provision of this Agreement is declared or found to be illegal, invalid, unenforceable or void by a court of competent jurisdiction, then (a) the validity, legality and enforceability of such provision as applied to any other particular facts or circumstances, and the other provisions of this Agreement, will not in any way be affected or impaired thereby, and (b) such provision will be enforced to the maximum extent possible so as to effect the intent of the parties.

13.4   Assignment. Neither Party may assign this Agreement or any of its rights or obligations under this Agreement, by operation of law or otherwise, without the prior written consent of the other Party, provided that Ripple may assign this Agreement and any of its rights and

19

RPLI_SEC 0095231

rippleLabs

obligations under this Agreement in connection with a merger, acquisition or sale of all or substantially all of its assets related to the Ripple Software or in connection with a corporate restructuring or reorganization. Any purported assignment made in violation of this Section 13.4 will be deemed to be, and will be, void. This Agreement will bind each Party and its permitted successors and assigns.

13.5   Governing Law; Venue. The validity, interpretation, construction and performance of this Agreement will be governed by the laws of the State of California, without giving effect to any choice of law rule. The Parties expressly and irrevocably disclaim and waive the application of the United Nations Convention on Contracts for the International Sale of Goods to this Agreement and to any claims arising under or related to this Agreement. Any legal suit, action or proceeding arising out of or relating to this Agreement will be commenced in a district court of the Northern District of California or in a state court in the County of San Francisco, California, and each Party hereto irrevocably submits to the exclusive jurisdiction and venue of any such court in any such suit, action or proceeding.

13.6   Injunctive Relief. Each Party acknowledges that a breach of its obligations under this Agreement, including, without limitation, its obligations set forth in Sections 2.5, 5 or 8 would cause irreparable damage to the other Party. Accordingly, each Party agrees that in the event of such breach or threatened breach, in addition to remedies at law, the other Party will have the right to injunctive or other equitable relief to prevent the first Party's violations of their obligations hereunder without the necessity of posting any bond or security.

13.7   No Waiver. No course of dealing, course of performance or failure of either Party strictly to enforce any term, right or condition of this Agreement will be construed as a waiver of any other term, right or condition. No waiver of any default or breach of any provision of this Agreement will be construed to be a waiver of any subsequent default or breach of the same or any other provision.

13.8   Relationship of the Parties. This Agreement will not be construed as creating an agency, partnership, joint venture or any other form of association, for tax purposes or otherwise, between the Parties, and the Parties will at all times be and remain independent contractors. Except as expressly agreed by the Parties in writing, neither Party will have any right or authority, express or implied, to assume or create any obligation of any kind, or to make any representation or warranty, on behalf of another Party or to bind another Party in any respect whatsoever. Ripple Services will retain sole control over the manner and means by which the Services are performed, reserves the right to determine the assignment of its personnel, and may engage third parties in the performance of the Services.

13.9   Notices. Any notice, request, demand or other communication required or permitted hereunder will be in writing, will reference this Agreement and will be deemed to be properly given: (a) when delivered personally; (b) when sent by facsimile, with written confirmation of receipt by the sending facsimile machine; (c) five (5) business days after having been sent by registered or certified mail, return receipt requested, postage prepaid; or (d) two (2) business days after deposit with a private industry express courier, with written confirmation of receipt. All notices will be sent to the address set forth on the signature page of this Agreement and to the notice of the person executing this Agreement (or to such other address or person as may be designated by a Party by giving written notice to the other Party pursuant to this Section 13.9). Notice will be considered effective when received, or if not received by reason of fault of addressee, when delivered.

20

RPLI_SEC 0095232

rippleLabs

13.10   Entire Agreement. This Agreement, any exhibits and schedules attached to it (including without limitation all Statements of Work) and any other terms and conditions expressly incorporated by reference herein, contains the entire understanding of the Parties with respect to the subject matter hereof, and supersedes and merges any and all related prior or contemporaneous understandings, agreements, representations, negotiations and discussions (including any standard form documentation of either Party), whether oral or written between the Parties relating to the subject matter hereof and all past courses of dealing or industry custom. This Agreement cannot be supplemented, modified, amended, released or discharged except in a writing signed by the duly authorized representative of both Parties. Notwithstanding the foregoing, the provisions of this Agreement shall not act to modify any applicable license or other terms regarding any Ripple Technology or Ripple Products that are contained in any separate license or agreement provided with or applicable to such Ripple Technology or Ripple Products, and in the event of a conflict, the terms of such separate agreement shall control.

13.11   Counterparts. This Agreement may be executed (including, without limitation, by facsimile or PDF signature) in one or more counterparts, with the same effect as if the Parties had signed the same document. Each counterpart so executed will be deemed to be an original, and all such counterparts will be construed together and will constitute one Agreement.

13.12   Interpretation. All captions and headings in this Agreement are for the purposes of convenience only and will not affect the construction of interpretation of any of the provisions of this Agreement. Any references to Articles, Sections and Exhibits are to be construed as references to the Articles or Sections of, and Exhibits to, this Agreement, unless otherwise indicated. The singular includes the plural, and the plural includes the singular. The term "or" is not exclusive. All references to "hereof," "herein," "hereunder," and other similar compounds of the word "here" will mean and refer to this Agreement as a whole rather than any particular part of the same. The terms "include" and "including" are not limiting.

13.13   General Use. Neither the Ripple Products nor any of the components of the Ripple Products are specifically developed or licensed for use in any nuclear, aviation, mass transit or medical application or in any other inherently dangerous applications. Neither Ripple nor its suppliers will be liable for any claims or damages arising from such use.

13.14   No Export. Integrator agrees to comply fully with all relevant export laws and regulations, including, without limitation, the laws and regulations of the United States and any other applicable country, to ensure that neither the Ripple Technology nor any direct product thereof is (a) exported, directly or indirectly, in violation of such export laws, or (b) intended to be used for any purposes prohibited by the export laws, including, without limitation, nuclear, chemical or biological weapons proliferation.

13.15   Rights and Remedies. All rights and remedies hereunder will be cumulative, may be exercised singularly or concurrently, and will not be deemed exclusive except as expressly provided in this Agreement. If any legal action is brought to enforce any obligations hereunder, the prevailing Party will be entitled to receive its attorneys' fees, court costs and other collection expenses, in addition to any other relief it may receive.

13.16   Non-Solicitation. During the Term and for one (1) year following the earlier of the expiration or termination of this Agreement thereof, neither Party will directly solicit for hire any employee of the other Party whose work involves the use, maintenance or development of the Ripple Software or Ripple Products (in the case of Integrator) or the Integrator Software or Integrator Products (in the case of Ripple); provided, however, this obligation will not apply to or

21

rippleLabs

be breached by (a) advertising of open positions, participating in job fairs and comparable activities, or other forms of soliciting candidates for employment or contract opportunities that are general in nature, (b) responding to unsolicited inquiries about employment or contract opportunities or possibilities from headhunters or other agents, or (c) responding to unsolicited inquiries about employment or contract opportunities from any individual.

[SIGNATURE PAGE FOLLOWS]

IN WITNESS WHEREOF, the Parties hereto have caused their respective duly authorized representatives to execute this Agreement as of the Effective Date.

Ripple Labs, Inc.   **[Integrator]**

By: _____   By: _____
Print Name: Print Name:
Print Title: Print Title:

Ripple Services, Inc.

By: _____
Print Name:
Print Title:

Ripple   Notice   Integrator   Notice
Address: 300 Montgomery Street   Address:
                 12th Floor
                 San Francisco, CA 94104
                 USA
Telephone: Telephone:
Fax: Fax:

22

rippleLabs

MASTER SOFTWARE AND SERVICES AGREEMENT

This Master Software and Services Agreement (the "**Agreement**") is entered into as of June __, 2015 (the "**Effective Date**") by and between Ripple Labs, Inc., a Delaware corporation ("**Ripple Labs**"), **Ripple Services, Inc.**, a Delaware corporation ("**Ripple Services**" and together with Ripple Labs, "**Ripple**"), and [BANK] ("**Bank**"). Ripple and Bank are each referred to hereinafter as a "**Party**" and collectively as the "**Parties.**"

RECITALS

Ripple Labs has developed various software, API's, services and related technology to facilitate access to and interaction with a decentralized network that permits currency exchange and payment transfers (the "**Ripple Protocol**"). Ripple Services provides custom implementation, development and support services for settlement and exchange solutions using the Ripple Protocol. Bank is interested in obtaining the right to use certain Ripple Products and Ripple Technology (both terms as defined below) including the right to provide access to such technology to its clients through the Banks' software and systems. Ripple Labs has agreed to license Bank to use the Ripple Products and Ripple Technology as provided herein. The Parties wish to further set forth the terms under which Ripple Services will provide integration, consulting and other services to support Bank's efforts hereunder.

NOW, THEREFORE, in consideration of the mutual covenants and agreements hereinafter set forth, the Parties do hereby agree as follows:

1.   **Definitions**

      1.1   "**Affiliates**" of an entity mean any corporation, company or other entity controlled by, controlling, or under the common control with such entity. For purposes of this definition, "control" means the direct or indirect ownership of more than fifty percent (50%) of the shares of the subject entity entitled to vote in the election of directors (or, in the case of an entity that is not a corporation, for the election of the corresponding managing authority) more than fifty percent (50%) interest in the income of such entity.

      1.2   "**Client**" means a person, company or other legal entity (i) who accesses the functionality, features or output of the Ripple Products in connection with the Bank Products either as a product and/or as a service for the Client to use, or (ii) for whom the Ripple Products are used by Bank on such Client's behalf.

      1.3   "**Confidential Information**" has the definition set forth in Section 7.1.

      1.4   "**Derivative**" means, with respect to a party's Technology, any translation, modification, upgrade, customization, enhancement, adaptation, improvement, compilation, abridgment or other form in which an existing work may be recast, transformed or adapted, including a derivative work, and any material derived from or improving upon existing trade secret material or Technology.

      1.5   "**Documentation**" means instructions, technical data, specifications, and other documentation, including programmer documentation, flow charts, logic diagrams, pseudo code, notations and other writings supporting the applicable Technology.

1

rippleLabs

1.6   **"Intellectual Property Rights"** means patent rights, design rights, mask work rights, copyrights, trade secret rights, and any other form of protection afforded by law to inventions, models, designs, works of authorship, databases or technical information and applications therefor.

1.7   **"Losses"** means losses, damages, penalties, demands, judgments, expenses and costs of any kind whatsoever, including reasonable attorneys' fees and expenses.

1.8   **"Bank Products"** means the software, hardware, services and other Technology of Bank or its Clients, including the Bank Technology, as well as the Intellectual Property Rights therein or related thereto. Bank Products do not include Ripple Products or Ripple Technology integrated with such Bank Products.

1.9   **"Bank Technology"** means any Technology developed, acquired or licensed by Bank or its Clients, including Bank Developed Technology, Bank Background Technology and Bank Derivative Technology (as such terms are defined in Section 4).

1.10   **"Ripple API"** means the application programming interface library that facilitates access to the Ripple Protocol and that may be used by the Bank Products.

1.11   **"Ripple Products"** means the software, hardware, services and other Technology made available by Ripple to Bank or Clients, including the Ripple Software and Ripple Technology, and access to the Ripple Protocol, as well as the Intellectual Property Rights therein or related thereto.

1.12   **"Ripple Software"** means the Ripple API and other software and related Ripple Documentation, as well as any Updates thereof, delivered pursuant to this Agreement, including any source code provided by Ripple.

1.13   **"Ripple Technology"** means any Technology developed, acquired or licensed by Ripple, including Ripple Developed Technology, Ripple Background Technology and Ripple Derivative Technology (as such terms are defined in Section 4).

1.14   **"Statement of Work"** means a written document detailing certain services and activities of the Parties that references this Agreement and that has been mutually agreed upon by the Parties.

1.15   **"Technology"** means creations, ideas, inventions, improvements, know-how, concepts, algorithms, protocols, data, processes, procedures, methods, systems, code, software, hardware, machines, prototypes, documents, components, and other materials, information and works of authorship, whether or not patentable, copyrightable, or susceptible to any other form of protection, including any Intellectual Property Rights in such items.

1.16   **"Term"** has the meaning set forth in Section 6.1.

1.17   **"Third Party Claim"** shall mean a claim by any person other than Ripple or Bank or their Affiliates, including claims by Clients.

1.18   **"Updates"** mean (1) all error corrections, bug fixes, or patches for the Ripple Software and related Ripple Documentation, and (2) all enhancements, modifications, improvements, and upgrades for the Ripple Software and/or related Ripple Documentation that improve the performance of the Ripple Software or that add new functionality or features.

2

rippleLabs

2.   **License of Ripple Products**

2.1   Grant of License by Ripple. Subject to the terms and conditions herein, Ripple hereby grants to Bank a limited, non-exclusive, non-transferable, right and license during the Term of this Agreement: (a) to access and use the Ripple Software (including related Ripple Documentation and Ripple Technology) to integrate the functionality of the Ripple Products into the Bank Products; (b) to make the Ripple Products available to Clients through the Bank Products subject to the terms of this Agreement; and (c) to use and permit Clients to use the Ripple Products to access the Ripple Protocol and other Ripple Products and communicate with the distributed Ripple Protocol network on behalf of itself and its Clients.

2.2   Scope of License. Bank may only use the Ripple Products for its own internal business purposes, including support of its Clients. In connection with the license granted in Section 2.1, Bank may copy, modify and adapt the Ripple Software solely for the purpose of incorporating or integrating the functionality of the Ripple Products into the Bank Products (provided, however, that Bank shall not reverse engineer the Ripple Software). Bank may copy or duplicate the Ripple Software for normal operational and backup purposes and as is necessary for the performance of its activities hereunder. Bank, however, will not:

(a)   distribute copies of any part of the Ripple Software or Ripple Documentation to Clients, provided that Bank may make the Ripple Documentation available to Clients as part of Client Documentation as permitted under Section 2.6;

(b)   make any Ripple Product available as a stand-alone application;

(c)   embed, incorporate, merge or combine the Ripple Products into any software, program, application, services, firmware or other hardware except for the Bank Products as explicitly permitted in this Agreement;

(d)   fork any part of the Ripple Software;

(e)   make the Ripple Products available to any third party other than a Client for whom all applicable Fees have been paid;

(f)   use third parties to private label, redistribute, resell or otherwise make available to Clients the Bank Products that include the Ripple Product functionality.

(g)   remove or obscure any proprietary notices (including any copyright, trademark, service mark, or patent designations), legends, labels, symbols, or logos from any Ripple Products;

(h)   sell, assign, lease, rent, loan, distribute, transmit, publish or otherwise transfer or make available any Ripple Products (with or without charge) to any person, other than in accordance with this Agreement;

(i)   upload or incorporate any malicious code or otherwise use the Ripple Products to further any purposes which is illegal or otherwise contrary to the license granted in this Section 2; or

(j)   except as permitted by this Agreement, encumber any Ripple Products or permit any Ripple Products to become subject to any lien.

3

RPLI_SEC 0095237

ripple Labs

2.3   Access by Clients.

(a)   Bank shall be responsible for permissioning its Clients to access and use the Ripple Products integrated with the Bank Products. Bank will not make the Ripple Products available to third parties except to its Clients pursuant to a Client license agreement (a **"Client Agreement"**) that includes: (i) restrictions on use consistent with the rights granted herein, including prohibitions on distributing, modifying or creating derivative works of any Ripple Products; (ii) protections for the Intellectual Property Rights in Ripple Products under terms no less protective than the protections set forth in this Agreement; and (iii) limitations on Ripple's liability relating to use of Ripple Products on terms substantially similar to those herein; in each case Ripple need not be specifically named if such provisions inure to Ripple's benefit. Bank shall notify Ripple of each Client with whom it enters into a Client Agreement. Bank shall promptly notify Ripple if Bank becomes aware of any breach of any Client Agreement relating to the Ripple Products. Upon the termination of any Client Agreement, Bank will use commercially reasonable efforts to ensure the return or destruction of all copies of any part of the Ripple Documentation in such Client's possession or control, including all reproductions thereof.

(b)   Bank will cause each Client with whom it enters into a Client Agreement to execute and enter into a Ripple End User Agreement in the form attached hereto as Exhibit A. Bank will promptly provide Ripple with a copy of each such Ripple End User Agreement. Ripple may amend Exhibit A from time to time by giving Bank written notice and Bank will use the amended version with Clients on a going forward basis. Ripple will notify Bank of any breach of a material obligation related to the Ripple Products under any Ripple End User Agreement of which Ripple becomes aware.

2.4   Reservation of Rights. All rights with respect to the Ripple Products not specifically granted to Bank hereunder are reserved by Ripple, and Ripple Labs remains the owner of all right, title, copyright and interest in the Ripple Software and any copies of it. Bank acknowledges that its and its Clients' use of the Ripple Protocol and other Ripple Products shall be subject to all applicable terms and conditions established for such items from time to time.

2.5   Exclusivity. Subject to a Party's confidentiality obligations under Section 7 and to the other Party's Intellectual Property Rights, neither Party shall be prohibited from dealing with any client or customer or from commercializing (or ceasing commercialization of) any products or services as it sees fit.   Notwithstanding the foregoing, during the Term, Bank agrees that: (a) the Ripple Protocol shall be Bank's preferred blockchain solution for distributed currency exchange and fund transfers, and Bank will in good faith facilitate, encourage and recommend to its Clients to exclusively use the Ripple Protocol when, where and in ways practicable, provided that Ripple acknowledges that Bank cannot offer or assure the exclusive use of the Ripple Protocol by any particular Client and that Clients retain the right to make their own technology decisions; and (b) Bank will not, directly or indirectly (including through its Affiliates), without the written permission of Ripple engage in any Competing Activities or work with, control or participate in the business of any individual, firm, corporation, institution or company engaged in Competing Activities. **"Competing Activities"** means to design, specify, support, develop, integrate, market, promote, license, sell, distribute, or otherwise commercialize in any manner any product or protocol which is competitive with or a substitute for the Ripple Software or Ripple Protocol.

2.6   Creation of Client Documentation. Bank may incorporate reasonable and necessary information from the Ripple Documentation into end user documentation for the Bank Products

4

rippleLabs

that are to be provided to Clients (**"Client Documentation"**); provided that Bank will not incorporate any Ripple Confidential Information or other non-public information concerning the Ripple Products without the prior written consent of Ripple which may be withheld in Ripple's sole discretion. Bank may not use the Client Documentation other than in connection with the Bank Products and Ripple Products or distribute it to any third parties other than Clients.

2.7   Grant of License by Bank. Subject to the terms and conditions herein, Bank hereby grants to Ripple a limited, non-exclusive, non-transferable, royalty free right and license during the Term of this Agreement to access and use any Bank Products (including related Documentation) made available by Bank to perform the Services. Bank represents and warrants to Ripple that as of the Effective Date and continuing through the Term that it has the right and authority to grant the foregoing license.

2.8   Procurement. Unless otherwise agreed to in writing by the Parties, Bank will be solely responsible for obtaining all hardware and the operating software for such hardware necessary to use the Ripple Products and for paying all fees in connection therewith. In no event will Ripple have any responsibility, liability or obligation with respect to any such hardware, software or any problems experienced by Bank or Clients relating to the use of such hardware or software, including, but not limited to, any non-conformance of such hardware or software with the information available to developers of applications for operation on such hardware and software, or any viruses, bugs or other errors that may be resident in such software.

2.9   Approvals. Bank will obtain, at its own expense, all registrations, licenses and approvals from all authorities and agencies which may be needed in order for Bank to exercise its rights and perform its obligations under this Agreement and to enable use of the Bank Products (and associated Ripple Product functionality) by it and its Clients.

3.   **Services**

3.1   Statements of Work. Bank may request that Ripple provide consulting, support or other Services to Bank or Clients, including assisting Bank in creating, developing, implementing and testing the Ripple Product functionality associated with the Bank Products and for providing maintenance, support and other services with respect thereto.

(a)   Ripple Services will use commercially reasonable efforts to render the services as set forth in each Statement of Work between Ripple and Bank (collectively, **"Services"**), and deliver any deliverables which may be specified therein (**"Deliverables"**). Ripple Services will deliver the Services according to the specifications set forth in the applicable Statement or Work, or developed thereunder as part of the Services (the **"Specifications"**). Ripple Services shall use reasonable efforts to complete the Services in accordance with the applicable schedule(s) contained in the Statement of Work. Services and the Deliverables will be considered accepted (**"Acceptance"**) upon delivery unless the Statement of Work sets forth an alternative Acceptance process.

(b)   Ripple shall have no obligation to perform Services until and unless it accepts a Statement of Work in writing. The Statement of Work will be in a form to be agreed between the Parties and will set forth the type and scope of work to be performed, project timeline and milestones, acceptance criteria and fees owed for the Services. Any such Statement of Work will reference, form a part of, and be governed by the terms of this Agreement.

5

rippleLabs

(c)   Bank shall reimburse Ripple for expenses incurred in connection with the Services as specified in the Statement of Work. Unless otherwise specified in a Statement of Work, Services are provided on a time and materials basis, and any budgets or estimated hours or costs in a Statement of Work are non-binding estimates only. Ripple will notify Bank as soon as it becomes aware that an estimate will be exceeded and agrees not to exceed estimated fees absent written and signed approval (but shall not be required to continue to provide Services until additional fees are approved). In the event of a conflict between the terms of a Statement of Work and this Agreement, the terms of this Agreement will control, unless the Statement of Work explicitly specifies that the conflicting provision will control.

(d)   Either Party may request a change a modification to the Services and/or Deliverables (a **"Change Request"**). fA Change Request shall be made in writing and shall be delivered to the other Party. The Parties will review the proposed changes and determine the effect that the implementation of the change will have on price, schedule and other terms and conditions of the affected Statement of Work. Upon completion of the review and acceptance of the Change Request, any changes in price, schedule or other terms will be documented. A Change Request shall become effective upon execution by both Parties and the Parties shall amend the applicable Statement of Work to reflect the Change Request before Ripple Services implements the Change Request. In no event shall Ripple be penalized for delays caused by a Change Request or be obligated to accept work proposed pursuant to a Change Request.

3.2   Support and Maintenance Services. Ripple Services will provide Bank with bug fixes, telephone support, Updates and other maintenance and support Services for the Ripple Products as set forth in a Statement of Work (**"Support Services"**) in exchange for the Fees specified therein. Except as otherwise set forth in a Statement of Work, Ripple will not be required to provide on-site Support Services.

(a)   Updates. Support Services will include Updates that are generally released to Ripple's clients who are receiving Support Services. Ripple shall have the sole discretion to determine which and when Updates are developed and released. Any Update provided to Bank will be included in the term "Ripple Software." If Ripple provides an Update to Bank which is identified as being intended to correct errors, increase performance or mitigate risk and/or the legal liability of either Party, Bank shall use reasonable efforts to insure that the Bank Products are modified to use such Updates and that its Clients receive the benefits of the Update. Bank agrees to use commercially reasonable efforts to make necessary changes to the Bank Products to accommodate Updates and new versions of the Ripple Products within three (3) months of Ripple providing the final specifications of such Upgrades and new versions to Bank. Ripple will provide development support reasonably required by Bank to facilitate such changes to the Bank Products.

(b)   Beta Releases. As part of Support Services, Ripple will notify Bank of pre-release alpha or beta versions of Updates to the Ripple Products. Upon Bank's request, Ripple will make such pre-releases reasonably available to Bank, at no additional cost, for review, evaluation, training, and planning purposes. Ripple will make good faith efforts to make each such pre-release available to Bank no later than the earliest date Ripple makes such pre-releases available to any other client. All such pre-releases are provided "**AS IS**," without warranty of any kind.

6

rippleLabs

    (c)   Client Support.   Ripple will provide Bank with telephonic, email and remote assistance in supporting Clients and the Ripple Product functionality associated with the Bank Products (e.g., Level 2 Support) as further detailed in a Statement of Work. Unless otherwise set forth in a Statement of Work, as between the Parties, Bank will be solely responsible for providing Clients with maintenance and support of the Bank Products (and related Ripple Products) (e.g., Level 1 Support), as well as with related training, installation and other technical and professional services. Upon mutual agreement of the Parties in a Statement of Work, Bank may subcontract with Ripple for the performance of certain of these Support Services. For each Client to whom Ripple provides Support Services, Bank will pay Ripple the Fees set forth in the Statement of Work. Notwithstanding any provision of this subsection, in the event a Client contacts Ripple directly regarding first-line support of the Ripple Products functionality associated with Bank Products, Ripple may respond directly to the Client or refer the Client to Bank, but in any case will inform Bank of the nature of Client's request, Ripple's recommendations, the actions taken, and results.

    3.3   Training Services. Bank will be responsible to provide training services to Clients. If requested by Bank, Ripple will provide training for the Ripple Products to Bank's implementation staff and technical support personnel as provided in a Statement of Work.

    3.4   Implementation and Training Services. Unless otherwise set forth in a Statement of Work, as between the Parties, Bank will be solely responsible to provide installation and other technical and professional services to Clients, including conducting all activities required to enable access to the Bank Products (and associated Ripple Product functionality) at its Client's locations and for providing training to such Clients. Bank will maintain a staff of capable technical personnel who have adequate ability to: (a) provide accurate information to Clients concerning the features and capabilities of the Ripple Products as associated with the Bank Products; and (b) provide technical assistance, support and maintenance to Clients in connection with the Bank Products and their interaction with Ripple Products as provided herein.

    3.5   Certification Services. If specified in a Statement of Work, the functionality of the Ripple Products used with the Bank Products will be certified prior to being connected to the Ripple Protocol production environment and prior to making the Ripple Products functionality available to any Client for production use. In order to be certified, the functionality must perform in all material respects in accordance with Ripple's internal testing requirements as mutually agreed by the Parties as set forth in a mutually agreed Statement of Work ("Conformance Testing"). Bank shall make the Bank Products available for Conformance Testing by a mutually agreed, commercially reasonable method, provided that, in all cases the Bank shall have the right to control Ripple's access to the Bank Products during any such Conformance Testing and that nothing in this provision shall require Bank to reveal any information or materials, the revelation of which would cause Bank to forfeit the protection of any Intellectual Property Rights or breach an obligation of confidentiality to any party with respect to such information or materials. The Services of Ripple in performing the Conformance Testing, if any, including any applicable charges, will be detailed in a Statement of Work. Upon the completion of the Conformance Testing and no later than five (5) days after the end of the relevant testing period as defined in the applicable Statement of Work, Ripple will notify Bank in writing of any non-conformities or defects found. Once all identified non-conformities or defects have been corrected the Bank Products will be resubmitted for additional Conformance Testing, and the process of testing, notification and correction will repeat until all

7

                    RPLI_SEC 0095241

rippleLabs

non-conformities and defects have been corrected or eliminated as evidenced by written acknowledgment signed by Ripple.

3.6   Cooperation. Bank will provide, in a timely and professional manner and at no cost to Ripple, full assistance and cooperation as may be reasonably requested by Ripple Services to enable the Services to be performed, including the provision of information and data which is complete and accurate; the provision of sufficient access to any equipment, computers, networks (including, VPN access), programs, files, documentation, test data, and sample outputs; and the provision of a suitable work environment when on-site. Ripple Services will not be liable for any deficiency in performing the Services if such deficiency results from Bank's (or a Client's) failure to provide such cooperation. Ripple Services' representatives will comply with reasonable written rules and regulations of Bank or a Client with respect to on-site work, provided that such rules and regulations are provided to Ripple Services prior to commencement of the Services.

3.7   Personnel. If in Bank's reasonable opinion, one of Ripple's personnel is not acting in a professional manner, is violating any of the requirements stated herein, or is failing in his or her performance of the Services, Bank may request that such individual be replaced, and Ripple Services will take commercially reasonable efforts to replace such individual as promptly as possible. Ripple Services agrees to take commercially reasonable efforts to maintain the continuity of Ripple personnel assigned to provide Services hereunder, however Ripple may replace personnel when necessary and appropriate upon written notice to Bank.

4.   **Ownership of Technology and Intellectual Property.**

4.1   Definitions.

(a)   **"Bank Background Technology"** means all Technology that Bank or any of its Affiliates or Clients: (i) has developed, acquired or licensed prior to the Effective Date, or (ii) develops, acquires or licenses entirely independently of its activities under this Agreement and without any reference to any information, data, materials, Ripple Technology or Ripple Confidential Information. Notwithstanding anything to the contrary herein, all Bank Derivative Technology will be deemed to be Bank Background Technology.

(b)   **"Bank Derivative Technology"** means any Technology (including works of authorship, materials, software, HTML, writings, drawings, designs, and specifications in which such Technology is embodied) that is conceived, created or otherwise developed by or for either Party or a Client (alone or with others) and that is a Derivative of the Bank Background Technology. Bank Derivative Technology does not include improvements, modifications, customizations or derivatives of the Ripple Background Technology or any Ripple Derivative Technology.

(c)   **"Bank Developed Technology"** means all Technology that Bank or any of its Affiliates, Representatives or Clients conceives, creates or otherwise develops during the performance of any activities relating to the Services under this Agreement, but excluding any Ripple Background Technology and Bank Background Technology.

(d)   **"Ripple Background Technology"** means all Technology that Ripple or any of its Affiliates: (i) has developed, acquired or licensed prior to the Effective Date, or (ii) develops, acquires or licenses entirely independently of its activities under this

8

ripple Labs

Agreement and without any reference to any information, data, materials, Bank Technology or Bank Confidential Information. Notwithstanding anything to the contrary herein, (1) all Ripple Derivative Technology will be deemed to be Ripple Background Technology, and (2) for the avoidance of doubt, Ripple Background Technology will be deemed to, and will, include the Ripple Software.

(e)   **"Ripple Derivative Technology"** means: (i) any Technology (including works of authorship, materials, software, HTML, writings, drawings, designs, and specifications in which such Technology is embodied) that is conceived, created or otherwise developed by or for either Party or a Client (alone or with others) and that is a Derivative of the Ripple Background Technology (including the Ripple Software); and (ii) any suggestions or proposals regarding new or improved features, functionality or performance of the Ripple Products.   For example, as defined in this Agreement, the data output of Ripple Software when employed by Bank or third party software program would *not* transform that software program into "Ripple Derivative Technology" merely because it employs the output of the Ripple Software as permitted under this Agreement. Likewise, any software code utilized to link the Bank Software and Ripple Software will not serve to constitute Ripple Derivative Technology if it does not contain any portion of Ripple Software.

(f)   **"Ripple Developed Technology"** means all Technology that Ripple or any of its Affiliates or Representatives conceives, creates or otherwise develops during the performance of any activities relating to the Services under this Agreement, but excluding any Ripple Background Technology and Bank Background Technology.

4.2   Background and Developed Technology. As between the Parties, Bank will own and retain ownership of all right, title, and interest in and to all Bank Background Technology and Bank Developed Technology. Ripple does not acquire any rights, express or implied, in any Bank Background Technology or Bank Developed Technology, other than those expressly specified in this Agreement, if any. As between the Parties, Ripple Labs will own and retain ownership of all right, title, and interest in and to all Ripple Background Technology and Ripple Developed Technology. Bank does not acquire any rights, express or implied, in any Ripple Background Technology or Ripple Developed Technology, other than those expressly specified in this Agreement.

4.3   Derivative Technology. Bank agrees to disclose promptly in writing and deliver to Ripple Labs all Ripple Derivative Technology that it conceives, creates or develops. All Ripple Derivative Technology will be considered Ripple Background Technology and the sole and exclusive property and Confidential Information of Ripple Labs. Except as set forth in this Agreement, Bank retains no rights to use the Ripple Derivative Technology and agrees not to challenge the validity of Ripple Labs' ownership in the Ripple Derivative Technology. All Bank Derivative Technology will be considered Bank Background Technology and the sole and exclusive property and Confidential Information of Bank.

4.4   Assignment and Further Assurances. To the extent that a Party retains rights in any Technology, Intellectual Property Rights or other items in contravention of the allocation of ownership set forth in this Section 4, such Party (the "**Assigning Party**") agrees to and hereby grants, assigns and conveys to the other Party (the "**Owning Party**") all of the Assigning Party's right, title and interest, if any, in such items and in all patents, copyrights, moral rights and other Intellectual Property Rights associated therewith ("**Conveyed Rights**").

9

rippleLabs

(a)   To the extent, if any, that any Conveyed Rights are not assignable or the Assigning Party retains any right. title or interest in and to any such items, the Assigning Party: (i) unconditionally and irrevocably waives the enforcement of such Conveyed Rights, and all claims and causes of action of any kind against the Owning Party with respect to such Conveyed Rights; (ii) agrees, at the Owning Party's request and expense, to consent to and join in any action to enforce such Conveyed Rights; and (iii) hereby grants to the Owning Party a perpetual, irrevocable, fully paid-up, royalty-free, transferable, sublicensable (through multiple levels of sublicensees), exclusive, worldwide right and license to use, reproduce, distribute, display and perform (whether publicly or otherwise), prepare derivative works of and otherwise modify. make, sell, offer to sell, import, use and exploit (and have others exercise such Conveyed Rights on behalf of the Owning Party) all or any portion of such Conveyed Rights, in any form or media (now known or later developed). Assigning Party further irrevocably waives any "moral rights" or other rights with respect to attribution of authorship or integrity of such Conveyed Rights that it may have under any applicable law. Assigning Party hereby waives and quitclaims to the Owning Party any and all claims, of any nature whatsoever, which Assigning Party now or may hereafter have for infringement of any Conveyed Rights therein assigned and/or licensed hereunder to the Owning Party.

(b)   Each Party agrees to cooperate fully, both during and after the Term, with the other Party for the purpose of securing, reserving, sustaining, perfecting and protecting a Party's ownership as set forth in this Section 3, including executing such written instruments as may be prepared by Owning Party and doing, at the Owning Party's expense, such other acts as may be necessary in the opinion of Owning Party to obtain a patent, register a copyright, or otherwise enforce Owning Party's rights in such Conveyed Rights {and Assigning Party hereby irrevocably appoints Owning Party and any of its officers and agents as its attorney in fact to act for and on Assigning Party's behalf and instead of Assigning Party, with the same legal force and effect as if executed by Assigning Party).

5.   Fees and Payment

5.1   Fees. Bank will owe fees to Ripple (**"Fees"**) for the use and/or license of the Ripple Technology and the provision of Services by Ripple as set forth in each Statement of Work. Bank shall reimburse Ripple for expenses incurred in connection with the Services as specified in an Statement of Work. All payments made under this Agreement will be in U.S. currency. All Fees are payable within thirty (30) days of the end of each calendar month in which they accrue and will be accompanied by the reports set forth in Section 5.2. Except as otherwise set forth in this Agreement, all fees or other charges will be payable thirty (30) days from the date of invoice. If Bank fails to pay any outstanding invoice within sixty days of issuance, it will be charged and agrees to pay a late payment fee equal to an annual rate of twelve percent (12%). Such a late payment fee will be calculated on a monthly basis and will be cumulative.

5.2   Reports and Audit. In connection with and at the time of each payment of any Fee, Bank will submit to Ripple Services a report that contains sufficient information necessary for Ripple Services to determine whether Bank is paying the correct Fee, including such information as specified in any fee schedule in a Statement of Work and information regarding each Client for whom a Fee is owed. During the Term of this Agreement and for one year thereafter, Ripple may, upon request, audit any and all work, billing or expense records of Bank relating to actual or

10

⁂rippleLabs

potential Fees; provided, however, that such audit shall occur only after reasonable notice to Bank and shall not unreasonably interfere with Bank's business or operations.

5.3   Taxes. All federal, state, local, value-added, transfer, sales and use taxes arising out of this Agreement will be paid by the Party required to pay such taxes under applicable law. The Party that is required by applicable law to make the filings, reports or returns and to handle any audits or controversies with respect to any such taxes will do so, and the other Party will cooperate with respect thereto as necessary. All Fees due under this Agreement will be made without any deduction or withholding, unless such deduction or withholding is required by any applicable law of any relevant governmental revenue authority then in effect.

5.4   Pricing of Bank Products and Services. Bank will be free to establish the amounts for all fees it charges to its Clients for the Bank Products and to otherwise control the terms and conditions on which it does business with its Clients; provided however that: (a) any Client Agreement includes the minimum terms and conditions as expressed in Section 2.2, and (b) Bank remains responsible for and pays all Fees and costs for Bank's and Clients' use of Ripple Products as provided hereunder.

6.   **Term and Termination**

6.1   Term. The term of this Agreement ("**Term**") shall continue for a period of three (3) years from the Effective Date, and shall automatically renew for additional one (1) year terms, unless either Party notifies the other in writing of its decision not to renew at least ninety (90) days prior to the end of the initial term or renewal term.

6.2   Termination for Cause. Either Party shall have the right to terminate this Agreement with immediate effect if the other Party becomes insolvent, or if the other Party materially breaches this Agreement and fails to cure such breach within sixty (60) days or receipt of written notice thereof.

6.3   Termination for Convenience. Each Party may terminate this Agreement without cause by providing at least ninety (90) days' prior written notice to the other Party.

6.4   Effect of Termination.

(a)   Bank may continue to use Ripple Products as part of the Bank Products beyond the termination of this Agreement for the benefit of a Client, provided: (i) the Client is not in breach of its Client Agreement, (ii) the use is consistent with the terms of this Agreement as if this Agreement were not terminated, (iii) the Client Agreement was entered into prior to the date of termination, (iv) the Client Agreement is not extended by amendment or renewal (over which the Bank has control) after the termination of this Agreement, and (v) Ripple is provided with any Fees and reports associated with such continued use as if the Agreement were not terminated. If requested by Bank, Ripple shall continue to provide Support Services pursuant to any Statement of Work existing as of termination in connection with authorized Client use continuing beyond termination, subject to Bank continuing to provide reports and payments of monies due Ripple for such Support Services. Notwithstanding the foregoing, the right to access Ripple Products and receive Support Services under this Section 6.4(a) shall terminate upon the earlier of (1) such time as an associated Client Agreement expires or terminates, or (2) two (2) years from the date of termination of this Agreement.

11

rippleLabs

(b)   Subject to Section 6.4(a), in the event of a termination or expiration of this Agreement, (a) all licenses and rights granted to the Parties hereunder will terminate, except as expressly set forth herein; (b) all Statements of Work will immediately terminate, and (c) each Party will return or destroy all Confidential Information of the other Party as provided in Section 7.5. Within thirty (30) days after termination or expiration of this Agreement, Bank shall return any tangible materials and Ripple Technology provided to Bank by Ripple, except for the Ripple Technology required to support, maintain, or provide related services to then-existing Clients of the Bank Products in accordance with Section 6.4(a). Upon termination of this Agreement Bank agrees to cease marketing, licensing and otherwise making the Ripple Products available to new clients or prospective clients.

7.   **Confidentiality And Non-Use**

7.1   Confidential Information. By virtue of this Agreement, a Party may have access to information that is confidential or proprietary ("**Confidential Information**") to the other Party or a Client. For purposes of this Agreement, "Confidential Information" of a Party means Technology, information, ideas, materials or other subject matter of such Party (including with respect to Bank, its Clients), whether disclosed orally, in writing or otherwise, that is provided under circumstances reasonably indicating that it is confidential or proprietary. Confidential Information includes, but is not limited to, all business plans, strategies and pricing data; methodologies, algorithms, protocols and analytical routines; software code, APIs and technical information; customer and supplier lists; Intellectual Property Rights; and financial information or materials; in each case, disclosed or otherwise provided by one Party (the "**Disclosing Party**") to the other Party (the "**Receiving Party**"). Without limitation of the foregoing, (i) all Bank Software and Bank Technology will be deemed to be Confidential Information of Bank, and (ii) all Ripple Software and Ripple Technology will be deemed to be Confidential Information of Ripple Labs. Any confidential or proprietary information of Clients to which Ripple has access in connection with this Agreement shall be deemed the Confidential Information of Bank protected under this Section 7. Bank acknowledges and agrees that transactions initiated within the Ripple Protocol will be available to the public on the Internet via the Ripple Protocol public ledger and shall not be considered Confidential Information under this Agreement.

7.2   Restrictions on Use. A Receiving Party shall not use Confidential Information of the Disclosing Party for any purpose other than in furtherance of this Agreement and the activities described herein. Bank is expressly prohibited from using or allowing or disclosing to any third parties to use, any of the Confidential Information of Ripple in any way to design, develop, market, promote, distribute, or otherwise exploit any products or services owned or developed by Bank or any third party which compete with the Ripple Products or any portion thereof. The Receiving Party shall not disclose Confidential Information of the Disclosing Party to any third parties other than those Affiliates, employees, advisors, contractors, agents or Clients who have a legitimate need to know such Confidential Information ("**Representatives**"). Each Party agrees that its Representatives shall be bound to retain the confidentiality of Confidential Information under provisions (including provisions relating to nonuse and nondisclosure) no less restrictive than those required for Confidential Information hereunder (in the case of Representatives that are not employees of the Receiving Party such agreement shall be in a writing signed by such Representatives). A Receiving Party shall be responsible for any misuse or disclosure of Confidential Information, or any other breach of this Agreement, by any of its Representatives as if Receiving Party had effected such act or omission itself. A Receiving Party shall protect Confidential

12

rippleLabs

Information of the Disclosing Party using reasonable care and commercially reasonable information safeguards. A Receiving Party shall advise the Disclosing Party in writing of any misappropriation or misuse of Confidential Information of the Disclosing Party of which the Receiving Party becomes aware.

7.3   Exclusions.   This Agreement imposes no obligation upon a Receiving Party with respect to the Confidential Information that the Receiving Party can show: (a) was already in the Receiving Party's possession at the time it was acquired from the Disclosing Party; (b) is or becomes publically available other than as a result of any action or inaction of the Receiving Party or its Representatives; (c) is lawfully obtained by the Receiving Party from a third party without a duty of confidentiality; or (d) is independently developed by the Receiving Party without use of or reference to the Disclosing Party's Confidential Information. In addition, this Section 7 shall not prevent the Receiving Party from disclosing Confidential Information of the Disclosing Party to the extent required by a judicial order or other legal obligation, provided that, in such event, the Receiving Party shall promptly notify the Disclosing Party to allow intervention (and shall cooperate with the Disclosing Party) to contest or minimize the scope of the disclosure (including application for a protective order).

7.4   Terms of This Agreement.   Notwithstanding anything to the contrary in this Agreement, except to the extent otherwise required by law, neither Party will disclose the terms of this Agreement to any third party without the express prior written consent of the other Party; provided, however, that either Party may disclose the terms of this Agreement to its attorneys and accountants or any potential investor or acquirer of a substantial part of such Party's business or assets, whether by merger, sale of assets, sale of stock or otherwise, or as otherwise may be required by law.

7.5   Return of Confidential Information.   Upon termination of this Agreement, each Party (as Receiving Party) will immediately return to the Disclosing Party all Confidential Information of the Disclosing Party embodied in tangible (including electronic) form or, at the Disclosing Party's discretion, destroy all such Confidential Information and certify in writing to the Disclosing Party that all such Confidential Information has been destroyed; provided that electronic data shall be subject to a Party's normal backup destruction policies.

7.6   Survival.   Any provisions of this Agreement, which are intended by their specific terms or by necessary implication, to survive the expiration or termination of this Agreement will so survive. Without limitation to the generality of the foregoing, Sections 4, 5.2, 6.4, 7, 8.3, 9, 10 and 12 will survive the termination or expiration of this Agreement.

8.   **Warranties**

8.1   Representations and Warranties.   Each Party represents and warrants to the other Party that as of the Effective Date and continuing through the Term: (i) it is not precluded by any existing arrangement, contractual or otherwise, from entering into this Agreement and performing hereunder; and (ii) it has the full right, power and authority to enter into this Agreement and to carry out its obligations hereunder and grant the rights granted by it hereunder, and there are no impediments known to it which would prevent its compliance with all the terms of this Agreement.

8.2   Service Warranty.   Ripple shall, during the 30 day period following Acceptance of a Service or Deliverable, fix any material non-conformance with the Specifications which Client identifies, and, on an interim basis, promptly provide any appropriate workarounds, or refund the fees paid, if any, for the deficient Service or Deliverable; provided, however, that Ripple will be

13

rippleLabs

excused from its performance to the extent that any Technology, data, information, materials or assistance provided, directly or indirectly, by or on behalf of Bank to Ripple to enable Ripple to perform the Services contains errors or defects, cannot be used to perform the Services or is insufficient or unsuited to enable Ripple Services to perform the Services. THE FOREGOING REMEDY WILL CONSTITUTE RIPPLE'S ENTIRE LIABILITY, AND BANK'S SOLE AND EXCLUSIVE REMEDY, WITH RESPECT TO RIPPLE'S FAILURE TO PERFORM THE SERVICES OR PROVIDE DELIVERABLES CONFORMING TO THE SPECIFICATIONS. Bank acknowledges that all Services are to be provided by Ripple Services and that Ripple Labs will not be liable for providing Services hereunder.

8.3   Disclaimers. EXCEPT AS PROVIDED IN THIS SECTION 8, THE RIPPLE PRODUCTS AND ANY OTHER MATERIALS, INFORMATION AND SERVICES PROVIDED BY RIPPLE TO BANK AND CLIENTS ARE PROVIDED "AS IS," AND TO THE MAXIMUM EXTENT PERMISSIBLE BY LAW, RIPPLE PROVIDES NO, AND HEREBY EXPRESSLY DISCLAIMS, ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING ANY IMPLIED WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE, ACCURACY AND NON-INFRINGEMENT, AND ALL WARRANTIES THAT MAY ARISE OUT OF COURSE OF DEALING, COURSE OF PERFORMANCE OR USAGE OF TRADE IN CONNECTION WITH THE SERVICES OR RIPPLE PRODUCTS OR OTHERWISE. IT IS THE RESPONSIBILITY OF BANK TO EVALUATE THE ACCURACY, COMPLETENESS AND USEFULNESS OF ALL DATA AND RESULTS GENERATED THROUGH ITS RECEIPT OF THE SERVICES OR RIPPLE PRODUCTS OR USE THEREOF.

9.   **Indemnification**

9.1   Ripple Indemnification.

(a)   Ripple Services will indemnify, defend and hold Bank and its Affiliates and each of their employees, officers, directors and agents harmless from and against any and all Losses suffered, incurred or sustained by any of them, or to which any of them become subject, as a result of any Third Party Claim arising from or in connection with: (i) any failure by Ripple or its Affiliates to comply with applicable laws; (ii) any breach by Ripple or its Representatives of any warranty or obligation of this Agreement; or (iii) any claim of personal injury or tangible property damage caused by any gross negligence or willful misconduct of Ripple or its Representatives during the provision of the Services.

(b)   Ripple Services will have no liability for any Third Party Claim to the extent that any Third Party Claim is based upon or attributable to: (1) any act, neglect, default or liability of Bank or its Affiliates or their directors, officers, managers, employees, agents, consultants or Representatives; (2) misuse, abuse or neglect of the Ripple Products or Services by any party other than Ripple; (3) use of other than the then-current, unaltered version and release of the applicable Ripple Products or Services; (4) use, modification, operation or combination of the Ripple Products or Services with any other products or services not provided or approved by Ripple; (5) Bank's failure to fully comply with this Agreement, the Documentation and any other reasonable instructions of Ripple; (6) any data, information, materials Technology or Intellectual Property Rights provided, directly or indirectly, by or on behalf of Bank to Ripple; (7) any problems or issues with any third party hardware, software, telecommunications systems or any other materials (including third party software contained in or provided along with the Ripple Products or Services); or (8) any actions or omissions of a Client or any third party participant in the Ripple Protocol network.

14

rippleLabs

9.2   Bank Indemnification.

(a)   Bank will indemnify, defend and hold Ripple and its Affiliates and each of their employees, officers, directors and agents harmless from and against any and all Losses suffered, incurred or sustained by any of them, or to which any of them become subject, as a result of any Third Party Claim arising from or in connection with: (i) the marketing, promotional and/or advertising activities of Bank and its Representatives in connection with the Bank Products; (ii) unauthorized representations or warranties made by Bank or its Representatives regarding the Ripple Products; (iii) any failure by Bank or its Affiliates to comply with applicable laws; (iv) any allegations that the Bank Products (excluding any part of the Ripple Products integrated therewith) or any Bank Technology, infringes or misappropriates a third party's intellectual property or other proprietary rights; (v) any unauthorized use, misuse, abuse or neglect of the Ripple Products by Bank or its Representatives; (vi) any breach by Bank or its Representatives of any warranty or obligation of this Agreement; (vii) any claim brought by any Client, including any claim regarding the use or inability to use the Bank Products or any Ripple Products integrated therewith, other than any Third Party Claim resulting from a breach of this Agreement by Ripple; and (viii) any claim of personal injury or tangible property damage caused by any gross negligence or willful misconduct of Bank or its Representatives.

(b)   Bank will have no liability for any Third Party Claim to the extent that any Third Party Claim is based upon or attributable to any act, neglect, default or liability of Ripple, its directors, officers, managers, employees, agents, consultants or Representatives, including any modification or use of the Bank Products by Ripple in a manner that Bank did not authorize or any use by Ripple of the Bank Products in combination with a product or service that Bank did not recommend or approve.

9.3   Indemnification Procedure.   A person asserting indemnification rights against a Party with respect to a Third Party Claim must: (a) give such Party prompt written notice of such Third Party Claim (provided that any delay in such notice will not relieve the indemnifying Party from its obligations to the extent it is not prejudiced thereby); (b) permit such Party to control the defence of such Third Party Claim and the negotiation of any settlement, provided, however, that the indemnifying Party may not agree to settle any Third Party Claim in a manner that adversely affects the indemnified Party without the consent of the indemnified Party; and (c) cooperate with such Party in such defense and negotiation at the indemnifying Party's expense. The indemnification rights of the Parties under this Section are their sole and exclusive remedies with respect to any Third Party Claims described herein.

10.   **Limitation of Liability and Damages**

10.1   NEITHER PARTY GUARANTEES THAT ACCESS TO ITS SOFTWARE OR PRODUCTS, OR INFORMATION AVAILABLE THROUGH ITS PRODUCTS, WILL BE UNINTERRUPTED, THAT SUCH ITEMS WILL BE FREE OF VIRUSES OR OTHER HARMFUL COMPONENTS OR THAT SUCH ITEMS CANNOT BE HACKED, TAMPERED WITH OR MALICIOUSLY ACCESSED BY THIRD-PARTIES.

10.2   NEITHER PARTY WILL BE LIABLE FOR ANY INDIRECT, EXEMPLARY, SPECIAL, CONSEQUENTIAL OR INCIDENTAL DAMAGES OF ANY KIND (INCLUDING LOST PROFITS AND DAMAGES FOR LOST DATA, LOST TRANSACTIONS, LOST ACCOUNTS AND WORK DELAYS), EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

15

rippleLabs

10.3   TO THE MAXIMUM EXTENT PERMISSIBLE BY LAW AND NOTWITHSTANDING ANYTHING IN THIS AGREEMENT TO THE CONTRARY OR ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY OR LIMITATION OF LIABILITY, RIPPLE'S AGGREGATE LIABILITY IN CONNECTION WITH THIS AGREEMENT, THE RIPPLE PRODUCTS OR THE SERVICES, REGARDLESS OF THE FORM OF ACTION GIVING RISE TO SUCH LIABILITY (WHETHER IN CONTRACT, TORT OR OTHERWISE) WILL NOT EXCEED THE AGGREGATE FEES ACTUALLY PAID BY BANK TO RIPPLE UNDER THIS AGREEMENT IN THE 12 MONTHS PRECEDING THE ACT OR OMISSION GIVING RISE TO THE CLAIM.

10.4   NOTWITHSTANDING ANYTHING TO THE CONTRARY, THE LIMITATIONS IN SECTIONS 10.2 AND 10.3 WILL NOT APPLY WITH RESPECT TO BREACH OF A PARTY'S CONFIDENTIALITY OBLIGATIONS HEREUNDER, INFRINGEMENT OF THE OTHER PARTY'S INTELLECTUAL PROPERTY RIGHTS, OR WITH RESPECT TO DAMAGES FOR WHICH A PARTY HAS AN OBLIGATION TO INDEMNIFY THE OTHER PARTY HEREUNDER. IN NO EVENT SHALL A PARTY HAVE LIABILITY OF ANY NATURE FOR CLAIMS TO THE EXTENT ARISING OUT OF ACTS OR OMISSIONS OF THE OTHER PARTY, ITS AFFILIATES, EMPLOYEES OR REPRESENTATIVES IN BREACH OF THIS AGREEMENT. THE LIMITATIONS OF LIABILITY CONTAINED IN THIS AGREEMENT ARE A FUNDAMENTAL PART OF THE BASIS OF EACH PARTY'S BARGAIN HEREUNDER, AND NEITHER PARTY WOULD ENTER INTO THIS AGREEMENT ABSENT SUCH LIMITATIONS.

11.   **Insurance**

11.1   Each Party will maintain at its own expense the following insurance:

(a)   **Workers' Compensation Insurance** including Occupational Disease and Employer's Liability in accordance with statutory limits with respect to all employees and agents entering upon the property of the other Party or its customers;

(b)   **General Liability Insurance** with a combined single limit of $2,000,000 per accident and $2,000,000 aggregate for bodily injury and property damage liability; and

(c)   **Products/Completed Operations Liability** (found under general liability) or **Errors and Omissions Professional Liability** with an aggregate limit of $2,000,000 covering liabilities arising out of products and services provided under this Agreement.

11.2   Each Party shall provide the other Party with a certificate of insurance evidencing such coverage and will name the other Party as an additional insured as its interests may appear within (15) days of signing this Agreement.

12.   **Miscellaneous**

12.1   Compliance with Applicable Laws. Bank agree to use Ripple Products in compliance with any applicable laws, rules or regulatory regimes (collectively, "**Laws**"), contracts, or third-party rights and agree not to engage in any transaction involving illegal products or services. Without limiting the foregoing, Bank agrees not to violate (a) any applicable domestic or foreign anti-corruption Law, including the United Kingdom Bribery Act of 2010 and the United States Foreign Corrupt Practices Act; (b) any applicable domestic or foreign Laws related to Anti-Money Laundering and anti-terrorist financing requirements, including the USA Bank Secrecy Act, as

16

rippleLabs

amended by the USA Patriot Act and the Financial Conduct Authority's Anti-Money Laundering Regulations; (c) the sanctions Laws administered by the U.S. Department of Treasury's Office of Foreign Assets Control; and (d) applicable export restrictions or Laws, or to cause Ripple to violate any such restrictions or Laws. Furthermore, Bank shall not utilize the Ripple Products in a manner that could cause Ripple to violate any of the foregoing Laws or other applicable laws, rules or regulations to which Ripple is subject.

12.2   Publicity. Neither Party shall publicly use or display the name, trademarks, service marks or logos (collectively, **"Trademarks"**) of the other Party (the **"Brand Owner"**) without the Brand Owner's prior written consent, except for a joint press release as mutually agreed by the Parties regarding their relationship under this Agreement. A Party's use of the Brand Owner's trademarks shall comply with the Brand Owner's trademark guidelines (as may be provided by the Brand Owner from time to time) and all legal requirements applicable to such use. A Party will not use or register (with any governmental or other authority, local or foreign) any trademark or trade name identical with, or confusingly similar to, any of a Brand Owner's Trademarks without the prior written consent of the Brand Owner. If requested by a Brand Owner, the other Party agrees to publish any affiliation disclaimer requested by the Brand Owner in a conspicuous manner and in a prominent location on affected materials.

12.3   Force Majeure. Except with respect to Bank's obligation to make timely payments, neither Party will be responsible for any delay or failure in performance to the extent that such delay or failure is caused by fires, strikes, embargoes, explosion, earthquakes, floods, wars, labor disputes, government requirements, civil or military authorities, acts of terrorism, acts of God or other causes beyond its reasonable control. In the event of such a Force Majeure condition extending for more than one hundred and thirty (30) days, the affected Party shall have the right, but not the obligation, to terminate this Agreement.

12.4   Severability. If any provision of this Agreement is declared or found to be illegal, invalid, unenforceable or void by a court of competent jurisdiction, then (a) the validity, legality and enforceability of such provision as applied to any other particular facts or circumstances, and the other provisions of this Agreement, will not in any way be affected or impaired thereby, and (b) such provision will be enforced to the maximum extent possible so as to effect the intent of the parties.

12.5   Assignment. Neither Party may assign this Agreement or any of its rights or obligations under this Agreement, by operation of law or otherwise, without the prior written consent of the other Party, provided that Ripple may assign this Agreement and any of its rights and obligations under this Agreement in connection with a merger, acquisition or sale of all or substantially all of its assets related to the Ripple Products or in connection with a corporate restructuring or reorganization. Any purported assignment made in violation of this Section 12.5 will be deemed to be, and will be, void. Subject to the foregoing, this Agreement will bind each Party and its permitted successors and assigns.

12.6   Governing Law; Venue. The validity, interpretation, construction and performance of this Agreement will be governed by the laws of the State of California, without giving effect to any choice of law rule. The Parties expressly and irrevocably disclaim and waive the application of the United Nations Convention on Contracts for the International Sale of Goods to this Agreement and to any claims arising under or related to this Agreement. Any legal suit, action or proceeding arising out of or relating to this Agreement will be commenced in a district court of the Northern District of California or in a state court in the County of San Francisco, California, and each Party hereto

17

rippleLabs

irrevocably submits to the exclusive jurisdiction and venue of any such court in any such suit, action or proceeding.

12.7   Injunctive Relief. Each Party acknowledges that a breach of its obligations under this Agreement, including its obligations set forth in Sections 2.2, 4 or 7 would cause irreparable damage to the other Party. Accordingly, each Party agrees that in the event of such breach or threatened breach, in addition to remedies at law, the other Party will have the right to injunctive or other equitable relief to prevent the first Party's violations of their obligations hereunder without the necessity of posting any bond or security.

12.8   No Waiver. No course of dealing, course of performance or failure of either Party strictly to enforce any term, right or condition of this Agreement will be construed as a waiver of any other term, right or condition. No waiver of any default or breach of any provision of this Agreement will be construed to be a waiver of any subsequent default or breach of the same or any other provision.

12.9   Relationship of the Parties. This Agreement will not be construed as creating an agency, partnership, joint venture or any other form of association, for tax purposes or otherwise, between the Parties, and the Parties will at all times be and remain independent contractors. Except as expressly agreed by the Parties in writing, neither Party will have any right or authority, express or implied, to assume or create any obligation of any kind, or to make any representation or warranty, on behalf of another Party or to bind another Party in any respect whatsoever. Ripple Services will retain sole control over the manner and means by which the Services are performed, reserves the right to determine the assignment of its personnel, and may engage third parties in the performance of the Services.

12.10   Notices. Except as otherwise provided in this Section, written notices and approvals under this Agreement shall be delivered by mail or email to the other Party's primary contact specified in the applicable Statement of Work, or as otherwise directed by the other Party in writing. Legal notices under this Agreement must be delivered in writing to the address set forth on the signature page of this Agreement (or to such other address or person as may be designated by a Party by giving written legal notice to the other Party pursuant to this Section) and will be deemed delivered: (a) when delivered personally; (b) when sent by facsimile, with written confirmation of receipt by the sending facsimile machine; (c) when sent by registered or certified mail, return receipt requested, postage prepaid; or (d) when sent by private industry express courier, with written confirmation of receipt. Notice will be considered effective when received, or if not received by reason of fault of addressee, when delivered.

12.11   Entire Agreement. This Agreement, any exhibits and schedules attached to it (including all Statements of Work) and any other terms and conditions expressly incorporated by reference herein, contains the entire understanding of the Parties with respect to the subject matter hereof, and supersedes and merges any and all related prior or contemporaneous understandings, agreements, representations, negotiations and discussions (including any standard form documentation of either Party), whether oral or written between the Parties relating to the subject matter hereof and all past courses of dealing or industry custom. This Agreement cannot be supplemented, modified, amended, released or discharged except in a writing signed by the duly authorized representative of both Parties. Notwithstanding the foregoing, the provisions of this Agreement shall not act to modify any applicable license or other terms regarding any Ripple Products that are contained in any separate license or agreement provided with or applicable to Ripple Products, and in the event of a conflict, the terms of such separate agreement shall control.

18

rippleLabs

12.12   Counterparts.   This Agreement may be executed (including by facsimile or PDF signature) in one or more counterparts, with the same effect as if the Parties had signed the same document. Each counterpart so executed will be deemed to be an original, and all such counterparts will be construed together and will constitute one Agreement.

12.13   Interpretation. All captions and headings in this Agreement are for the purposes of convenience only and will not affect the construction of interpretation of any of the provisions of this Agreement. Any references to Articles, Sections and Exhibits are to be construed as references to the Articles or Sections of, and Exhibits to, this Agreement, unless otherwise indicated. The singular includes the plural, and the plural includes the singular. The term "or" is not exclusive. All references to "hereof," "herein," "hereunder," and other similar compounds of the word "here" will mean and refer to this Agreement as a whole rather than any particular part of the same. The terms "include" and "including" are not limiting.

12.14   General Use. Neither the Ripple Products nor any of the components of the Ripple Products are specifically developed or licensed for use in any nuclear, aviation, mass transit or medical application or in any other inherently dangerous applications. Neither Ripple nor its suppliers will be liable for any claims or damages arising from such use.

12.15   No Export.   Bank agrees to comply fully with all relevant export laws and regulations, including the laws and regulations of the United States and any other applicable country, to ensure that neither the Ripple Technology nor any direct product thereof is (a) exported, directly or indirectly, in violation of such export laws, or (b) intended to be used for any purposes prohibited by the export laws, including nuclear, chemical or biological weapons proliferation.

12.16   Rights and Remedies. All rights and remedies hereunder will be cumulative, may be exercised singularly or concurrently, and will not be deemed exclusive except as expressly provided in this Agreement. If any legal action is brought to enforce any obligations hereunder, the prevailing Party will be entitled to receive its attorneys' fees, court costs and other collection expenses, in addition to any other relief it may receive.

12.17   Non-Solicitation. During the Term and for one (1) year following the earlier of the expiration or termination of this Agreement thereof, neither Party will directly solicit for hire any employee of the other Party whose work involves the use, maintenance or development of the Ripple Products (in the case of Bank) or the Bank Products (in the case of Ripple); provided, however, this obligation will not apply to or be breached by: (a) advertising of open positions, participating in job fairs and comparable activities, or other forms of soliciting candidates for employment or contract opportunities that are general in nature, (b) responding to unsolicited inquiries about employment or contract opportunities or possibilities from headhunters or other agents, or (c) responding to unsolicited inquiries about employment or contract opportunities from any individual.

[SIGNATURE PAGE FOLLOWS]

19

rippleLabs

IN WITNESS WHEREOF, the Parties hereto have caused their respective duly authorized representatives to execute this Agreement as of the Effective Date.

Ripple Labs, Inc.   **[Bank]**

By: _____   By: _____
Print Name: Print Name:
Print Title: Print Title:

Ripple Services, Inc.

By: _____
Print Name:
Print Title:

Ripple Notice   Bank Notice
        Address: 300 Montgomery Street   Address:
                    12th Floor
                    San Francisco, CA 94104
                    USA
        Telephone: Telephone:
             Fax: Fax:

20

RPLI_SEC 0095254

Ripple Protocol Proof of Concept (POC)
Integration Statement of Work
Bank Name

Month 201X

ripple

TABLE OF CONTENTS

1 Introduction

This Statement of Work ("SOW") is entered into between Bank Name ("Partner") and Ripple Services, Inc. ("Company"), a wholly owned subsidiary of Ripple Holdings, dated "TBD", and consists of this SOW and its applicable attachments and documents referenced herein. The Parties acknowledge and agree that all references to Company in the Agreement or this SOW shall be deemed to include Ripple Service, Inc., and each of its Affiliates. For purposes of this Agreement, the term "Affiliate" shall mean an entity that controls, is controlled by, or is under common control with a party, where "control" means the direct or indirect ownership of more than 50% of the voting securities of such entity or party. In the event of any conflict, ambiguity or inconsistency between or among this SOW and the Agreement or any amendment, exhibit, schedule or other attachment thereto, the parties specifically acknowledge and agree that the terms and conditions set out in this SOW shall control. All other terms and conditions between the Parties shall remain unchanged and in full force and effect.

This POC Implementation SOW describes the tasks and responsibilities to be executed by Company and Partner to implement a limited-use cross border payment service on the Ripple protocol. This SOW identifies the work activities that will be monitored, defines the boundaries for scope control, identifies responsibilities, and clarifies many of the areas where issues can arise that need to be managed. Company's performance under this SOW depends on the Partner and its third parties performing its responsibilities, as set forth in this SOW. Parties may adjust timelines, when necessary, and to the extent required, to address the impact of changes to agreed designs by Partner or any failures by Partner or its third parties to complete its responsibilities in a timely manner.

The fees for this project are to be fixed fee and will cover all of the anticipated work necessary for Company to perform. Any additional work or modification to this document may have additional cost and an impact to the estimated timing.

RPLI_SEC 0095257

2 Scope of Work

2.1   Implementation Phases
    2.1.1   Phase I: Explore the Ripple technology through sending cross border transactions between Partner entities in Location 1 and Location 2. Develop a design and integration plan for a production implementation of a Ripple service
    2.1.2   Phase II: Build and rollout a production quality cross border payments service over Ripple. A separate Statement of Work and proposal will be created for this phase.

2.2   Partner will implement the capability to send payments manually between Partner entities in Location 1 and Location 2 via Ripple.

2.3   The Ripple POC Implementation will be structured to:
    2.3.1   Complete Phase I within 120 days of integration commencement.

2.4   Partner will send transactions to the Ripple protocol through a user interface developed by Ripple Labs.
    2.4.1   Partner will manually adjust house accounts when transferring funds into and out of Ripple.
    2.4.2   Partner will set up entities/accounts on Ripple according to best practices to minimize risk.
    2.4.3   Partner will serve as the Market Maker and will provide foreign exchange services for the transaction.

2.5   Partner will plan a production implementation of a Ripple service.
    2.5.1   Partner will develop a use case or cases for a production Ripple service, such as a B2B cross border payment service.
    2.5.2   Partner will document initial high-level production architecture to integrate Ripple Connect to the bank ledger system to facilitate automated transfers from customer accounts to Ripple.
    2.5.3   Partner will create a wireframe design for a user interface for the production Ripple service.
    2.5.4   Partner will create a production plan including cost and effort estimates to implement the production Ripple service.
    2.5.5   Partner will obtain signoff on the production plan, estimates, and designs from Partner business, legal, IT, security, risk, and compliance stakeholders and/or teams.

2.6   Company will assist the partner in activities referenced in 2.4 & 2.5

2.7   Company and Partner will negotiate a contract for the build, rollout, and ongoing support of the production-quality service built on Ripple

2.8   Meetings:
    2.8.1   Kickoff Meeting: Company and Partner will participate in a kickoff meeting within 10 days of the commencement of the POC Implementation.
    2.8.2   Project Meetings: Project meetings will be conference calls unless jointly decided otherwise. The Company Project Manager will be the primary liaison between Partner and Company and he/she will be the primary Company participant in joint (Partner and Company) project meetings. The Company Project Manager will use discretion in arranging for Ripple subject matter expert participation in topic-specific meetings as necessary (e.g., Product Management, Engineering, etc.).

2.9   Items **NOT** in the scope of the project are:
    2.9.1   Transactions other than CAD/USD are not included as a part of this SOW.
    2.9.2   Security Tests: Ethical hacks, application scanning, and vulnerability tests supported by Company are not included as a part of this SOW.
    2.9.3   Performance Tests: Performance or load tests supported by Company are not included as a part of this SOW. System performance will be assured as per the SLA (Service Level Agreement) incorporated in the Agreement between Company and Partner during a production implementation.
    2.9.4   Ongoing Customer Support: Support beyond the POC service is not included as a part of this SOW.

3 Assumptions and Prerequisites

3.1   Business Hours: Unless otherwise agreed, project participants will be available during their
        normal local office business hours.
      3.1.1   Company business hours: 9 am PST – 5 pm PST
      3.1.2   Partner business hours: 9 am EST – 5 pm EST

4   Deliverables

4.1   Company

    4.1.1   Training: Company will provide training to key stakeholders to introduce the Ripple technology and the Ripple product(s).

    4.1.2   Documentation: In addition to documentation provided on https://dev.ripple.com, Company will provide materials to support integration, which include:

        4.1.2.1   Cross Border Payment Tutorial

        4.1.2.2   High Level Payment Flow

        4.1.2.3   Sequence Diagram for Payment Flow

        4.1.2.4   Spec for Ripple Connect and Payment Services Protocol

        4.1.2.5   Spec for Ripple Stream

    4.1.3   Project Plan: In collaboration with Partner, Company will prepare and manage a Project Plan for the integration of Ripple services including all Company and Partner deliverables and will provide the Project Plan and updates to Partner as requested. Company time and cost estimates assume a Partner project team experienced with the relevant technology and development techniques.

4.2   Partner

    4.2.1   Project Plan: In collaboration with Company, Partner will prepare and manage a Project Plan for the integration of Ripple services including all Company and Partner deliverables and will provide the Project Plan and updates to Company as requested.

    4.2.2   Success Criteria: Partner will identify and document Project Success Criteria for evaluating project performance and whether to move forward with future stages of integration, if applicable. Company will assist in Success Criteria development, tracking, and evaluation.

    4.2.3   Production Ripple Service Plan: Partner will produce a Production Service Plan package that will receive signoff by key Partner stakeholders in Business, Legal, Risk, Compliance, IT, and Security. It will include the following documents that will produced by Partner with the support of Company:

        4.2.3.1   Business case or cases

        4.2.3.2   High level architectural design

        4.2.3.3   UI wireframe design

        4.2.3.4   Cost estimate

        4.2.3.5   Implementation plan for a production Ripple service

RPLI_SEC 0095260

5 Project Milestones and Delivery Timeline

5.1   Period of Performance: From Date – To Date
5.2   Schedule: To be revised in Project Planning. Example schedule below: (Note to Author: Create a new one here)

Task	Mar				Apr					May				Jun				Jul		
	1	2	3	4	1	2	3	4	5	1	2	3	4	1	2	3	4	1	2	3
Project Kickoff			▓	▓																
Project Planning			▓	▓																
Ripple Training					▓	▓														
Set up Development Environment					▓	▓														
Pilot Transaction Execution							▓	▓	▓	▓	▓	▓	▓	▓	▓	▓	▓			
Production Business Case Planning														▓	▓					
Production Design and Planning																▓	▓			
Pilot Stakeholder Demo and Production Plan Signoff																		▓	▓	

5.3   Dependencies: The project dependencies that have been agreed upon between Partner and Company for delivery are as follows:

Dependency	Delivery Date to Company
Identify participating banks for POC implementation	15 July 2015
Determine production business case(s)	31 August 2015
High level production architectural design	15 September 2015
UI wireframe design for production service	15 September 2015
Production implementation cost and effort estimate	21 September 2015
Implementation plan for production Ripple service	21 September 2015
Signoff on production Ripple service plan	30 September 2015

5.3.1 The Dependencies and Delivery Dates to Company may be amended and/or supplemented only by mutual agreement between the parties as a result of the detailed planning activity that produces the Project Plan.

5.3.2 The Dependencies outlined in this SOW and the Project Plan must be adhered to by Partner in order for Company to meet its delivery obligations.

5.3.3 If a Dependency is missed, then a Change Request will be raised and agreed to between the parties, acting in good faith. This will have the effect of resetting subsequent Milestones and Delivery Dates. It may also require amendment of the Partner Fees as outlined in Section 7 of this SOW.

6 Roles and Responsibilities

6.1   Key Company Personnel
The Company will provide the following personal to help facilitate the success of the POC:

Project Manager: Lead Engineer:
Name   Name
Email   Email

Business Lead:
Name
Email

6.2   Key Partner Personnel
The Partner will provide the following personal to help facilitate the success of the POC:

Project Manager: Lead Engineer:
Name   Name
Email   Email

Business Lead:
Name
Email

7 Cost

7.1   Integration Service Fee: $ ███████ USD
    7.1.1   Fixed fee for up to four months from the project kick off date
7.2   Fees after four months will be on a T&M basis
7.3   Company will pay T&E expenses, if any

8   Change Management

8.1   The following Change Management Process will be used to identify, record, assess and approve changes to this SOW. Company and Partner will follow this process to classify, rank, approve, or reject changes. Change Management requests must be clearly defined and will include cost and schedule implications.

   8.1.1   Any changes to the work identified in this SOW, including but not limited to any changes in scope, customization, integration, resources, or timing as defined in this SOW or in the Application Services Agreement will require the change to be documented, estimated, and approved by both Company and Partner prior to any work commencing on the change.

   8.1.2   The scheduling of Company work resulting from an approved Change Management request will be based on availability of Company resources, and will be completed on a best effort basis.

9 SOW Acceptance

This Statement of Work is subject to the terms and conditions of the Application Service Provider Agreement. Except as otherwise noted in this document, this Statement of Work represents the entire agreement between the parties with respect to the subject matter of this Statement of Work, supersedes all other negotiations, agreements, contracts, representations, proposals, commitments, and understandings, oral and written, with respect thereto, and does not operate as acceptance of, and will prevail over, any conflicting terms, conditions and provisions of any other instrument of a party. Any amendment to this Statement of Work must be in writing and signed by a duly authorized representative of Partner and Company.

Partner and Company agree that any requirements introduced after this Statement of Work is executed will be subject to the aforementioned Change Request Process.

Ripple Services, Inc.   **Partner Name**

By: _____   By: _____

Name: _____   Name: _____

Title: _____   Title: _____

Date: _____   Date: _____

10 Appendix A – Legal Terms and Conditions

1. <u>Fees and Taxes</u> Partner will pay the fees for work actually performed at the rates set out in, and for expenses accrued as set out herein; there are no other fees or costs to be paid by Partner to Company. The fees exclude all applicable taxes and Partner will pay and Company will remit same to all applicable taxing authorities as required by law. Partner will be entitled to withhold all applicable withholding taxes from the fees and to remit same to applicable taxing authorities as required by law.

2. Intellectual Property Rights

    a. Each party will own all right, title and interest in and to all of its Background Technology (including all intellectual property rights in and under all of the foregoing).

    b. Each party will own all right, title and interest in and to any improvements, modifications and other derivative works to its Background Technology, including any customizations made to its existing code or solution by either party (collectively the "Derivative Technology"). Such Derivative Technology created by either party will be and will be deemed to be part of the underlying Background Technology.

    c. "Background Technology" will mean technology that: (i) a party has already developed prior to the performance of any activities related to the SOW, or (ii) such party develops entirely independently of its activities under the definitive agreement and without any reference to any information, data or other materials provided by the other party.

    d. Neither party will copy, modify, create improvements or derivative works of, adapt, translate, reverse engineer, disassemble or decompile the other party's proprietary software, or attempt to extract any materials and/or exploit any intellectual property rights embodied in the other party's proprietary software except to the extent permitted to perform the party's obligations in relation to the SOW.

    e. Except with respect to Derivative Technology, each party will own any work product, inventions, technology, designs, machines, code, software, documentation, data, materials, works and intellectual property that is conceived, created, developed discovered, reduced to practice or fixed in a tangible medium by such party in connection with this Agreement.

    f. To the extent that a party retains rights to any materials, technology, or intellectual property in contravention of the allocation of ownership set forth in this Section 2, such party (the "Assigning Party") agrees to and hereby grants, assigns and conveys to the other party all of the Assigning Party's right, title and interest, if any, in such items and in all patents, copyrights, moral rights and other intellectual property rights associated therewith. Each party agrees to promptly take, at the requesting party's expense, any actions or execute any documents that the other party reasonably requests to confirm or accomplish the allocation of ownership in Section 2.

    g. Except as explicitly provided herein, nothing in this Agreement will act to give a party any rights, license, or interest in the equipment, materials or intellectual property rights of the other party.

3. <u>Company Representations, Warranties, and Covenants</u>. Company represents, warrants and covenants to Partner the following:

    a. Each of the Deliverables and the Services, or any part thereof, does not and will not infringe or misappropriate the intellectual property rights of any person and the authors of each of the Deliverables have waived or will waive all moral rights which they may have therein;

    b. Company will not, without Partner's prior written consent, use Partner's premises for any purpose other than for providing the Services and will observe and cause its personnel to observe all applicable laws and policies while present in or on Partner's premises

4. <u>Confidentiality Covenant</u>. The parties have previously entered into a Non-Disclosure Agreement dated _____ (the "NDA") – a copy of which is attached hereto as Exhibit B and whose terms and conditions are incorporated into this SOW. For the avoidance of doubt, the Confidential and/or Proprietary Information to which

RPLI_SEC 0095267

a party has access pursuant to this SOW and any amendment thereto shall be protected in accordance with the terms of the NDA. The purposes for which the Confidential and/or Proprietary Information may be used under the NDA are hereby amended so that such purposes include the work and services to be provided under this SOW. The term of the NDA is hereby amended so that any Confidential and/or Proprietary Information disclosed during the term of this SOW shall be considered Confidential and/or Proprietary Information thereunder.

5. Term. This Agreement will commence on the Effective Date and will continue for the period set out in the SOW, unless terminated earlier by Partner in accordance with Section 6 hereof.

6. Termination. Notwithstanding Section 5, above, Partner will have the right to terminate all or any part of this Agreement forthwith upon ten (10) days prior written notice to the Company. Upon early termination, Company will be entitled to fair compensation based on the pro-rata portion of the fees specified in the SOW for Services already completed.

7. Survival. Any provision of this Agreement that expressly or by its nature survives termination or expiration of this Agreement, or that contemplates performance or observance subsequent to termination or expiration of this Agreement, including Section 4 above and the NDA, shall survive termination or expiry of this Agreement.

8. Governing Law. This Agreement will be governed by and construed in accordance with the laws of the State of California and the federal laws of the United States of America applicable therein.

9. Assignment. Company will not assign or subcontract all or any portion of this Agreement without the prior written consent of Partner.

10. Entire Agreement. This Agreement, together with the NDA, and any amendment thereof, constitutes the entire agreement between the Parties pertaining to the subject matter of this Agreement.

11. Publicity. As per the business terms in sec 7.8.3 of the SOW

12. Limit of Liability. Except as expressly provided in this Agreement, Company disclaims all warranties and representations, express or implied, regarding the Services and Deliverables, including but not limited to, all implied warranties of merchantability and fitness for a particular purpose. Partner's sole remedy in connection with deficient Services or Deliverables will be re-performance or re-delivery of the defective items. Partner will have sole liability for the use and operation of Services and Deliverables once they have been accepted and put into use. Except for Company's obligations under Section 3 and under Section 4 or the NDA, or for a party's infringement of the other party's intellectual property rights the liability of Company or Partner to the other for any breach of this Agreement or otherwise from any acts or omissions of its respective Personnel, will in all circumstances be limited to the direct damages not to exceed the amount of fees paid or payable to Company hereunder, and neither party will be liable for any claim by the other party or any other person for consequential, incidental, exemplary, punitive, or special damages, including lost data, lost profits, or business loss, arising out of the other party's performance or nonperformance under this Agreement, whether in contract, tort or other legal theory.

13. Audit Rights. Company will cooperate with Partner and/or its designee in fulfilling reasonable requests made in connection with Partner's vendor due diligence and audit functions and with regard to examinations by regulatory authorities.

Appendix 7 (Q31) — Copies of BSA/AML/OFAC Policies and Procedures on a Legal Entity Basis (6 Documents)

Ripple Trade, LLC
BSA/AML/OFAC Policy/Program – June 2015

Table of Contents

I

ripple

Ripple Trade, LLC
BSA/AML/OFAC Policy/Program – June 2015

INTRODUCTION

Ripple Trade, LLC (known herein as "Ripple Trade" or "the Company") is committed to ensuring that its products and services are not used to launder money, finance terrorism, evade US government sanctions or otherwise facilitate criminal activity. It is the policy of the Company to comply fully and continuously with Bank Secrecy Act/Anti-Money Laundering ("BSA/AML") and Office of Foreign Assets Control ("OFAC" or, more broadly, "sanctions") legislation and regulations. This Program outlines Ripple Trade's efforts to detect and deter money laundering and terrorist financing, and provides an overview of the major functions and responsibilities within the Company's BSA/AML/OFAC Program.

Ripple Trade, LLC was formed on May 28, 2015 in response to a Settlement Agreement with regulatory authorities to move the Ripple Trade Service, into an MSB registered with the U.S. Treasury's Financial Crimes Enforcement Network ("FinCEN")[1]. Ripple Trade registered with FinCEN as a money service business ("MSB") on June 2, 2015.

The Ripple Trade product is a web-based open-source software client (www.rippletrade.com) through which users can access the internet-based Ripple protocol and view balances (both fiat and virtual) using the Ripple Trade Service, held on the decentralized ledger. Neither the balances, the currency, nor a user's public or private keys are stored by either the Company or the Ripple Trade product - the interface simply allows users a convenient method to view and manage funds held on the Ripple protocol. The product provides a way for Ripple Trade users to access their funds, but is not in itself a way of storing of safeguarding funds. Ripple Trade has neither custody nor control of its users' funds, nor does it have the ability to initiate user transactions.

POLICY STATEMENT

Ripple Trade will comply with the BSA and all applicable money laundering and sanctions laws and regulations in all aspects of its business. This Policy applies to all employees, Board members, and service providers whose activities relate to any aspect of the BSA program.

The Policy establishes the following four pillars of BSA/AML compliance:
   o   The appointment of a qualified BSA/AML Officer ("BSA Officer");

---

[1] In May 2015, Ripple Labs and its wholly owned subsidiary XRP II entered into a Settlement Agreement with the Department of Justice and FinCEN.

2

ripple

RPLI_SEC 0095271

Ripple Trade, LLC
BSA/AML/OFAC Policy/Program – June 2015

o   The establishment of internal controls designed to limit money laundering and sanctions risks;
o   The delivery of annual BSA/AML and Office of Foreign Assets Control ("OFAC") training to employees, management, the Board and other applicable persons; and
o   The performance of independent testing of the BSA/AML and OFAC program.

SCOPE AND APPLICABILITY

The BSA/AML/OFAC Policy and Program applies to all Ripple Trade activities and all Ripple Trade personnel, as well as any service provider personnel whose activities impact the Policy and Program, are subject to compliance with prescribed requirements.

Ripple Trade recognizes that non-compliance can expose the Company to substantial risk and civil or criminal penalties. All employees are responsible for understanding this Program/Policy and undertaking specific responsibilities assigned to them. Absent advance approval in writing from the BSA Officer, no employee, or service provider has the authority to act contrary to the provisions of this Policy or to authorize, direct, or tolerate violations of the Policy by any other person.

Employee or service provider non-compliance with, or violation of, Program requirements may result in:

- Disciplinary action, up to and including termination of employment or service provider contract in appropriate cases;
    and/or
- Civil and/or criminal penalties.

Willful blindness, or "turning a blind eye," to a potential money laundering violations can expose both the Company and individuals to potential liability.

ROLES AND RESPONSIBILITIES

Below is a brief description of Ripple Trade roles and responsibilities with respect to BSA/AML/OFAC compliance:

3

Ripple Trade, LLC
BSA/AML/OFAC Policy/Program – June 2015

BSA Compliance Officer

Ripple Labs Chief Compliance Officer is the designated BSA Officer for Ripple Trade. BSA Officer responsibilities include:

o   Implementing and maintaining the BSA/AML/OFAC Program and Policy, and related procedures;

o   Developing a comprehensive 'Implementation Plan' to include all specified Settlement Agreement actions as well as items necessary to fully implement the BSA/AML/OFAC Program;

o   Providing quarterly reporting to Ripple Trade's Compliance Oversight Committee evidencing appropriate governance of Ripple Trade's BSA/AML/OFAC compliance program

o   Reviewing and refreshing the BSA/AML/OFAC Program and Policy, procedures, risk assessment, and any relevant training materials at least annually, or more frequently as circumstances require;

o   Maintaining training records as they relate to BSA/AML and OFAC training for Ripple Trade staff;

o   Reporting to Treasury and managing Ripple Trade's response to potential OFAC hits;

o   Overseeing execution of the Program, including KYC and suspicious activity monitoring/reporting activity, providing guidance and direction to Ripple Trade staff on effective Program implementation;

o   Ensuring that the Company adheres to timely AML and sanctions reporting, including designing appropriate controls and coordinating independent testing of their effectiveness;

o   Ensuring that all staff are knowledgeable regarding potential red flags and is aware of their responsibility to promptly report violations or potential suspicious activity through the escalation procedures described in this Program;

o   Reviewing any changes to AML and sanctions laws, regulations, guidance in consultation with regulatory advisors and outside counsel to ensure that the Company remains fully compliant with legal obligations and or regulatory expectations;

o   Promptly alerting the Compliance Oversight Committee and executive management to any material issues of BSA/AML/OFAC non-compliance, and instituting and monitoring corrective action;

o   Maintaining appropriate MSB registration and pursuing required money transmitter state licenses;

o   Projecting and implementing resource plans to ensure the Program can be effectively executed;

o   Conducting periodic monitoring/quality/assurance of BSA controls;

∴ ripple

4

RPLI_SEC 0095273

Ripple Trade, LLC
BSA/AML/OFAC Policy/Program – June 2015

> o   Periodically validating monitoring systems and parameters;
> o   Evaluating any new products and services for BSA/AML and OFAC risk and ensuring that Ripple Trade has sufficient controls in place to mitigate its risk prior to launch;
> o   Coordinating and ensuring that independent program testing takes place at least annually.

The BSA Officer is further responsible for:

> o   Presenting an BSA/AML/OFAC Program and corresponding risk assessment, as well as the BSA/AML/OFAC training Program to Ripple Trade's Compliance Oversight Committee for review and approval on a no less than annual basis;
> o   Reporting to Ripple Labs' Board of Directors annually on the approval of the BSA/AML/OFAC Program, the corresponding risk assessment, and all relevant BSA/AML/OFAC training materials by Ripple Trade's Compliance Oversight Committee;
> o   Providing semi-annual reporting to Ripple Labs' Board of Directors evidencing appropriate governance of the Ripple Trade's BSA/AML/OFAC Compliance Program;
> o   Providing BSA/AML/OFAC training to Ripple Labs' Board of Directors and Compliance Oversight Committee members on an annual basis, or more frequently, as needed; and
> o   Ongoing consultation with regulatory advisors and legal counsel to ensure that Ripple Trade's BSA/AML/OFAC Program remains current with applicable laws and leading industry standards.

Compliance Oversight Committee

Ripple Trade's Program is governed by a Compliance Oversight Committee that meets quarterly, or more frequently as needed. The Oversight Committee comprises the BSA Officer, the Ripple Labs General Counsel, and Ripple Labs Head of Regulatory Relations and Strategic Policy Initiatives. The Committee reports no less than semi-annually to the Ripple Labs Board of Directors. The Compliance Oversight Committee also maintains responsibility for oversight of necessary remediation of and enhancement to the BSA/AML/OFAC Program, which will initially include the Settlement remediation efforts and Risk Assessment actionable items but could, in the future, include self-identified issues as well as issues arising from independent testing or examinations.

The Compliance Oversight Committee is responsible for:

> o   Promoting and implementing a strong culture of compliance;

5

⋅⋮ ripple

Ripple Trade, LLC
BSA/AML/OFAC Policy/Program – June 2015

o   Ensuring that the Company appoints a suitably qualified BSA Officer with appropriate levels of staffing support;
o   Overseeing the BSA Officer (the BSA Officer will recuse herself from this responsibility);
o   No less than annually, approving this Policy, the BSA/AML/OFAC risk assessment and the BSA/AML/OFAC Training Program;
o   Establishing and communicating an appropriate risk tolerance for BSA/AML and OFAC risk;
o   Reviewing compliance reports and any compliance issues escalated to executive management, including mitigation plans;
o   Periodically reviewing the adequacy of compliance resources;
o   Reviewing periodic BSA/AML/OFAC compliance reports from the BSA Officer; and
o   Reviewing the results of independent testing and examinations, ensuring that Ripple Trade takes appropriate action to remediate or enhance its BSA Program taken, where indicated.

Company Employees

All Ripple Trade employees are fully accountable for:

o   Reviewing and understanding the BSA/AML/OFAC Program;
o   Escalating any unusual or potentially suspicious activity that they observe or detect in the normal course of business, to the BSA Officer, either through the designated escalation procedures;
o   Attending required AML training in accordance with Ripple Trade's BSA/AML/OFAC Training and Education Program;
o   Escalating actual or potential compliance weaknesses to the BSA Officer, and working with the BSA Officer to implement corrective action as needed:
o   Maintaining systems, controls, and reports that support BSA/AML and sanctions compliance efforts as directed by the BSA Officer;
o   As applicable, notifying and seeking the BSA Officer's approval for new or modified products or services; and
o   Otherwise assisting and complying with requirements of Ripple Trade's BSA/AML/OFAC Program and policy, as needed.

6

●❊ ripple

RPLI_SEC 0095275

Ripple Trade, LLC
BSA/AML/OFAC Policy/Program – June 2015

MINIMUM PROGRAM REQUIREMENTS

An effective BSA/AML/OFAC Program and Policy is essential to both achieving and demonstrating compliance with legal requirements. This BSA/AML/OFAC Policy is updated on an annual basis, or more frequently as circumstances warrant, and is presented annually by the BSA Officer to the Compliance Oversight Committee for review and approval. The Compliance Oversight Committee approved of this Program on June 6, 2015. The following provides an overview of Ripple Trade's Program; more detailed requirements are specified in the Policy section starting on page 15.

Designation of a BSA Compliance Officer

The Company has designated a BSA Officer to direct, implement, enforce, maintain, and update Ripple Trade's BSA/AML/OFAC Policy and Program.

The BSA Officer and all AML Compliance staff have full authority to access all company records and direct all company personnel as necessary to implement this Program.

Internal Controls:

Annual Risk Assessment

Ripple Trade's risk assessment is conducted annually, or more frequently as needed. Given the infancy of Ripple Trade's current BSA/AML/OFAC Program and the challenges associated with implementing controls in a non-traditional operating environment, Ripple Trade will re-assess its BSA/AML/OFAC risk within six months - by December 31, 2015.

The purpose of the risk assessment is to identify the Company's BSA/AML and OFAC risks, and assess implemented controls to meet the regulatory expectations for an MSB. The risk assessment forms the basis of Ripple Trade's annual BSA/AML/OFAC Program, and will:

- o Determine the Company's risk profile by assessing the inherent risks presented by the Ripple Trade product, its customer base and the geographies in which its customers operate;
- o Determine the adequacy and effectiveness of Company's controls;
- o Identify the existence of any insufficiently mitigated risk; and

7

◆🐧 ripple

Ripple Trade, LLC
BSA/AML/OFAC Policy/Program – June 2015

o   Recommend necessary actions to enhance the Company's BSA/AML/OFAC
    Compliance Program in order to mitigate and reduce residual risk to acceptable
    levels.

Ripple Trade's initial risk assessment takes the following into consideration:

o   Rating the inherent risk of Ripple Trade's products and services, its customer
    base and the geographies which it serves and in which its customers are located;
o   Identifying and assessing the adequacy of Ripple Trade controls in light of AML
    and OFAC requirements for money services businesses registered with FinCEN;
o   Rating the Company's residual risk in consideration of assessed controls; and
o   Identifying and assigning responsibility for any necessary control enhancements
    identified as a result of the risk assessment process.

Upon completion, the BSA Officer will present the risk assessment to the Compliance
Oversight Committee for review and approval. Additionally, the BSA Officer is
responsible for reporting to Ripple Labs' Board of Directors on the approval of each risk
assessment by executive management of Ripple Trade.

Identification, Verification and Screening, and Know Your Customer

Ripple Trade's Know Your Customer ("KYC") Program includes customer identification
and verification ("CIP") of all Ripple Trade users as well as risk-based enhance due
diligence ("EDD") for users with identified heightened BSA/AML/OFAC risk. Ripple Trade
is developing functionality to obtain and verify all required CIP for new and existing
users. Ripple Trade has, effective June 2, 2015, suspended onboarding new customers
until it has put this functionality in place. Ripple Trade expects to launch its user
verification and screening process in late June, 2015.

For individuals, to the extent feasible, Ripple Trade will verify user identities through
industry-standard automated non-documentary verification processes approved by the
BSA Officer.

Ripple Trade will conduct manual CIP verification for legal entities, which will also
include identification of ultimate beneficial owners of 25% or more. At the time of
obtaining and verifying CIP, screening against OFAC sanctions lists and screening to
identify any politically exposed persons (PEPs") requiring EDD, will also be conducted.

Access to the Ripple Trade service by existing users will be immediately and
systematically prevented if CIP cannot be automatically verified. Access will continue to
be disabled until AML Compliance has conducted successful manual verification. If CIP
cannot be verified manually, if EDD requirements cannot be fulfilled, or if OFAC

8

*ripple

RPLI_SEC 0095277

Ripple Trade, LLC
BSA/AML/OFAC Policy/Program – June 2015

screening identifies sanctioned persons access will continue to be disabled and appropriate action, such as SAR filing or OFAC reporting is conducted, as warranted. New users are prevented from accessing the Ripple Trade service until after such time as CIP is adequately verified, any EDD requirements are fulfilled, and OFAC screening is completed with no match results.

Monitoring, Reporting, and Information Disclosures

Ripple Trade conducts monitoring for suspicious activity and reports this activity as required by law. In addition to filing suspicious activity reports ("SARs"), law enforcement is notified of cases that specific agencies may have particular interest in. Ripple Trade responds as appropriate to requests for information from FinCEN and other governmental entities, and, where applicable, undertakes voluntary information sharing as provided in 31 C.F.R. § 314(b).

Control Testing

In addition to conducting routine internal and overseeing annual execution of external independent testing of the BSA/AML OFAC Program, the BSA Officer, or designated AML Compliance staff, is responsible for:

o   assessing the risk posed by any new products that Ripple Trade offers and for ensuring that the Company has developed implementing controls prior to launch; and

o   effective risk-based due diligence and oversight of critical third-party providers that operate, assist with, or provide support for any of Ripple Trade's controls for BSA/AML/OFAC processes.

Additionally, the BSA Officer, along with key members of the Compliance Oversight Committee, regularly consults with regulatory advisors and legal counsel to ensure that Ripple Trade's BSA/AML/OFAC Policy and Program remains current with applicable laws and leading industry standards

Training and Education

9

Ripple Trade, LLC
BSA/AML/OFAC Policy/Program – June 2015

The BSA Officer is responsible for ensuring that Ripple Trade employees and any other covered parties (including service provider personnel whose duties impact the Program) receive appropriate training on the requirements of the Company's BSA/AML/OFAC Policy and Program. The Company has established a Training and Education Program that details Ripple Trade AML training policy requirements and frequency of AML training for all Ripple Trade employees, new hires, and AML Compliance staff including the BSA Officer.

The Compliance Oversight Committee approves the Training Program no less than annually. Records of approval(s) are maintained centrally by Ripple Trade AML Compliance staff. The BSA Officer is responsible for providing BSA/AML/OFAC training to Ripple Labs Board of Directors and Compliance Oversight Committee members on an annual basis, or more frequently, if needed.

Management Reporting

The BSA Officer prepares quarterly BSA/AML/OFAC compliance reports for Compliance Oversight Committee review. Quarterly reports describe central Program activities, including remediation, corrective action, any key risk indicators, as well as any identified instances of suspicious activity, fraud or other wrongdoing.

The Chief Compliance Officer, in conjunction with the Company's Compliance Oversight Committee is also responsible for providing validation reporting to Ripple Labs Board of Directors evidencing appropriate governance of Ripple Trade's BSA/AML/OFAC Compliance Program on a semi-annual basis.

Recordkeeping

The Bank Secrecy Act ("BSA") establishes recordkeeping requirements related to various types of records, including customer accounts, and may impose other filing requirements needed to document a financial institution's overall compliance with the BSA. In general, the BSA requires financial institutions to maintain most records for at least five years. Records can be maintained in many forms including original, electronic, copy, or a reproduction. Ripple Trade is not required to keep a separate system of records for each BSA requirement; however, it must maintain all records in a way that makes them accessible within a reasonable period of time.

The Company maintains records of customer identity, verification in proprietary ID service databases. Due diligence and suspicious activity investigations and reports, as

10

ripple

Ripple Trade, LLC
BSA/AML/OFAC Policy/Program – June 2015

well as disclosures of information in response to governmental requests are maintained by AML Compliance on a dedicated, secure Compliance server. Additional records, as required by law, are also created and maintained by AML Compliance. This Program requires retention of all records for a minimum of five years, as well as retention of customer records for a minimum period of five years after the end of the customer relationship.

Money Transmission, Licensing and Registration

The BSA Officer is responsible for registration as a money services business with FinCEN and maintains the Company's federal registration and renewal as required by law. The BSA Officer, in consultation with legal counsel, is responsible for determining state licensing requirements resulting from its identified customer base and activities and applying for/maintaining licenses as necessary. The BSA Officer maintains responsibility for monitoring and initiating state license applications, where needed. The Company retains all documents regarding MSB or other money transmitter registration and state licensure indefinitely.

Agency Relationships

The Company does not have agents and will not establish any agency relationships. Should Ripple Trade decide to use agents at any time in the future, the Company shall establish and implement appropriate controls to comply with MSB agent requirements, including but not limited to the creation of a list of such agents and development of effective agent oversight mechanisms, in advance of pursuing the agency relationships.

Foreign Bank and Financial Accounts Reporting

Ripple Trade does not maintain a foreign bank account and therefore has no FBAR filing obligation. Should Ripple Trade decide at any time in the future to open and maintain a foreign bank account, the Company will establish controls to comply with FBAR reporting requirements in advance of opening the account.

11

ripple

Ripple Trade, LLC
BSA/AML/OFAC Policy/Program – June 2015

Currency, Sale and Transportation of Negotiable Instruments

The Company does not accept any form of physical currency (i.e., the coin or paper of the United States or any other government) from the public or its users, nor does it participate in the sale, transportation, or handling of negotiable instruments. Should Ripple Trade decide at any time in the future to accept, sell, or transport financial instruments, the Company will establish controls to comply with all relevant record-retention and reporting requirements.

Funds Transmittal Recordkeeping

In May, 2015, Ripple Trade submitted a request to FinCEN for an administrative ruling with respect to the applicability of Fund Transmittal Record-keeping and Travel Rule requirements to its operation. At this time, there is no established mechanism within the Ripple network to capture identity information nor is there a means to reliably identify when a Ripple Trade customer sends funds to a downstream financial institution and therefore triggers a Travel Rule obligation. Pending the requested ruling from FinCEN, this Program requires Ripple Trade to:

- o   maintain records of all items required by Fund Transmittal Recordkeeping that can be generated by its service; and
- o   make every effort to build functionality to:
    - • capture required information; and
    - • transmit required identifying information to other financial institutions, when required.

With respect to any single transaction or aggregated series of transactions from one individual or multiple individuals known to be acting in concert totaling more than USD $███ in a single day, the Company shall capture and retain the following records to the extent they exist within Ripple Trade's systems:

- o   the name and address of the Ripple Trade sender or receiver;
- o   the amount of the transaction;
- o   as much of the following information as is available: the name and address of the sender and/or recipient (if a Ripple Trade user); the Ripple address of the sender and/or recipient; and, any other specific identifier of the sender and/or recipient.

The Company will retain records of subject transactions for a minimum of five (5) years. Ripple Trade is not a dealer in currency; additional record-keeping in that respect is, therefore, not required.

12

Ripple Trade, LLC
BSA/AML/OFAC Policy/Program – June 2015

Cooperation with Law Enforcement

It is Company policy to cooperate to the extent permitted by applicable law and in accordance with its policies, with legal process or other requests for information or assistance received from law enforcement in accordance with established internal procedures governing responses to law enforcement requests.

The BSA Officer reviews all subpoenas and requests for information or assistance from law enforcement, consults with legal counsel prior to disclosing any information to determine whether it is permissible to provide the requested information or assistance, and then responds accordingly to law enforcement.

Records of law enforcement legal process and requests, and productions made in response will be retained for five (5) years.

Confidential records of law enforcement requests and productions are maintained and disclosed only:

o   as allowed by legal process;
o   within the Company or to outside counsel as necessary to comply with the request;
o   for legal advice; or
o   to prepare a responsive production.

National Security Letters ("NSLs")

Upon receipt, NSLs must be referred to the BSA Officer who consults with legal counsel prior to disclosure of any information. NSLs must be treated with the highest levels of confidentiality; the existence of a NSL will be disclosed only as necessary to comply with the requests contained in it. NSL records must be maintained confidentially and securely. The BSA Officer is responsible for responding to all law enforcement requests.

Records of NSLs and responsive documents are retained for a period of five (5) years.

Voluntary Information Sharing (Section 314(b))

In June 2015, the Company submitted notification to FinCEN confirming its participation in 314(b) information sharing program.

13

⋅⋅ ripple

RPLI_SEC 0095282

Ripple Trade, LLC
BSA/AML/OFAC Policy/Program – June 2015

Before undertaking any voluntary information sharing, the BSA Officer, or designee, must ensure that if the information is to be shared with the financial institution, that financial institution has filed the appropriate notice with FinCEN.

The BSA Officer, or appropriate designated AML Compliance staff, is responsible for handling and tracking all incoming 314(b) requests in accordance with established 314(b) procedures, as well as drafting and approving all outgoing 314(b) requests. The BSA Officer or designee will ensure that all outgoing requests and are limited exclusively to investigations of possible money laundering or terrorist financing. The BSA Officer will ensure that the information is used only for the following purposes:

o Identifying and, where appropriate, reporting on money laundering or terrorist activities;
o Determining whether to establish or maintain an account, or to engage in a transaction; or
o Assisting the sharing financial institution in complying with performing such activities.

If shared information reveals potential suspicious activity occurring through Ripple Trade, the BSA Officer will initiate an investigation, which may result in the filing of a SAR in accordance with this policy.

Records of information shared and information received will be retained for five (5) years. Any such records must be maintained confidentially and securely.

14

⣿ ripple

Ripple Trade, LLC
BSA/AML/OFAC Policy/Program – June 2015

BSA/AML/OFAC POLICY

INTERNAL CONTROLS

Customer Identification Program ("CIP") and Know Your Customer ("KYC") Activities

Ripple Trade has detailed procedures documenting the process of conducting CIP and KYC on customers, which are maintained in a separate document. As of June 2, 2015, Ripple Trade adopted CIP and KYC standards, and is in the process of implementing these for existing and new customers. Until such time as the new CIP process is implemented and existing Ripple Trade customers fully remediated, required user information may not be available for all users.

As of June 2015, access to Ripple Trade will not be permitted for any new users of Ripple Trade if CIP information cannot be appropriately verified through either automated non-documentary means or subsequent manual review and verification of additional/supplementary documentation requested by AML Compliance staff.

Due to the high inherent BSA/AML risk associated with virtual currency, the Company will conduct additional due diligence on all users including screening against OFAC sanctions lists (see OFAC section below) and screening to identify foreign politically exposed persons ("PEPs").

When necessary, for example, for shell companies, PEPs and other identified users subject to the enhanced due diligence requirements of this Policy, AML Compliance personnel will request the user to complete a KYC form that requires additional information, such as purpose of account, source of funds, expected activity, and detailed information on beneficial owners of 25% or more.

Identification requirements for individuals

Once the customer verification and screening application is launched in late June, 2015, all new Ripple Trade users must enter the following information through Ripple Trade's web-based user interface:

- o   Full legal name;
- o   Physical Address;
- o   Date of Birth; and

15

Ripple Trade, LLC
BSA/AML/OFAC Policy/Program – June 2015

    o Tax payer identification number (TIN) such as a social security number or other
government-issued identification number. Ripple Trade will require a SSN or TIN
for US citizens and permanent residents.

To the extent feasible, Ripple Trade will verify user identities through industry-standard
automated non-documentary verification processes approved by the BSA Officer. If this
information cannot be automatically verified as provided, the Ripple Trade user-
interface requires the user to upload a copy of a valid, government-issued photo
identification card such as a passport, driver's license or other form of identification
documents approved by the BSA Officer, supplemented by a recent document showing
proof of address in cases where the identification document does not incorporate the
physical address provided. A member of the AML Compliance Team will conduct
manual review of the submitted documentation.

A similar identification process is required for existing Ripple Trade users; however,
under the terms of the Settlement Agreement, an initial grace period (until October 30,
2015) is allowed for submission and verification of CIP information for existing users.
After this time, if user CIP information is not submitted, or cannot be appropriately
verified through automated or manual means, user access to Ripple Trade will be
disabled.

Identification requirements for entities

Non-individual users identified through the web-based Ripple Trade CIP interface
require manual identity verification by AML Compliance staff members. Once identified
as a non-individual entity, AML Compliance is responsible for contacting the customer to
obtain the following items for manual review and customer verification:

    o A completed KYC form including, but not limited to, information on source of
funds and expected activity through Ripple Trade;
    o Documents evidencing the legal existence of the entity, such as articles of
incorporation or other documentation approved by the BSA Officer[2];
    o Identifying information (name, address, and date of birth) for all ultimate
beneficial owners with 25% or more entity ownership;
    o Proof of address or existence of physical location of the entity.

---

[2] For all articles of incorporation and identity verification documentation presented that is not in English,
it is the responsibility of the customer to provide a third party translation. With the exception of proof of
address, which may be a utility bill, lease agreement, or other document with the user's name and
address, Ripple Trade will not accept documentation in a language other than English.

16

•❖ ripple

RPLI_SEC 0095285

Ripple Trade, LLC
BSA/AML/OFAC Policy/Program – June 2015

Verification procedures

AML Compliance staff is responsible for reviewing information and documentation provided for inconsistencies. Compliance personnel may also use other means of non-documentary verification approved by the BSA Officer, such as alternative online verification services, to verify customer identity if:

- o AML Compliance personnel are unfamiliar with the documents presented; or
- o the BSA Officer believes it will provide greater assurance about the identity of the customer.

The Company will not conduct business with any user who does not provide identification information. If a potential or existing user refuses to provide all requested CIP and KYC information, or appears to have intentionally provided misleading information, the Company will not enable access to the Ripple Trade service or otherwise establish a new user relationship, and, for existing customers will disable access to Ripple Trade. In such circumstances, the BSA Officer will determine whether the filing of a SAR is warranted, and document that decision.

AML Compliance is responsible for documenting Ripple Trade's user identification and verification process, the methods used, along with the results and resolution of any discrepancies. AML Compliance maintains records all documents relied upon to verify a user's identity. With respect to non-documentary verification, the Ripple Trade retains evidence of automated verification as well as a description of the methods and the results of any measures taken to conduct such verification.

The Company will retain records of required identification information obtained for Ripple Trade users for the duration of the relationship with the user and for a period of five (5) years after the user account is closed (or five (5) years from the date of the last user transaction through Ripple Trade.)

Prohibited Users

Ripple Trade will not support activity of entities prohibited by law or regulation such as:

- o entities that issue bearer shares;
- o any OFAC-sanctioned persons;
- o unauthorized on-line gambling companies;
- o shell banks;
- o persons featured on Section 311 Special Measures lists;
- o unlicensed financial institutions; and

17

ripple

Ripple Trade, LLC
BSA/AML/OFAC Policy/Program – June 2015

    o Any individual or entity undertaking, or with close ties to, activity contrary to U.S. law or regulation.

In addition, Ripple Trade will not onboard or terminate the customer relationship of any individual or entity the BSA Officer determines presents unacceptable AML or sanctions risks to the Company. This will include, but not be limited to, persons identified with prior convictions for financial-related crimes that indicate unacceptable risks of money laundering, terrorist financing and/or sanctions evasion.

The Company will prevent any new users identified as prohibited entities from signing up or otherwise accessing Ripple Trade. Should prohibited entities be identified through CIP/KYC remediation of existing Ripple Trade users, they must be immediately escalated to the BSA Officer for review, escalation, investigation, and ultimate termination.

Higher Risk Users

Ripple Trade subjects all higher-risk users to EDD according to the standards set down in the next section.

1. Politically Exposed Persons (PEPs)

Once the customer verification and screening application is launched in late June, 2015, all individual Ripple Trade users, both new and existing, are subject to screening against PEP lists to identify known PEPs. PEPs are generally defined as:

    o a **"senior foreign political figure"** - a senior official in the executive, legislative, administrative, military or judicial branches of a foreign government (whether elected or not), a senior official of a major foreign political party, or a senior executive of a foreign government-owned corporation. In addition, a senior foreign political figure includes any corporation, business, or other entity that has been formed by, or for the benefit of, a senior foreign political figure;

    o the **"immediate family"** of a senior foreign political figure typically includes the figure's parents, siblings, spouse, children, and in-laws;

    o a **"close associate"** of a senior foreign political figure is a person who is widely and publicly known to maintain an unusually close relationship with the senior foreign political figure, and includes a person who is in a position to conduct substantial domestic and international financial transactions on behalf of the senior foreign political figure.

Ripple Trade considers all PEPs to be high risk and subject to annual compliance reviews. Upon identification of a PEP, and prior to providing new user access to Ripple Trade, in

18

ripple

Ripple Trade, LLC
BSA/AML/OFAC Policy/Program – June 2015

addition to obtaining a completed KYC prior to onboarding, designated AML Compliance staff must request, review and evaluate information concerning:

o the potential user's background, income sources, source of funds and wealth and any other financial information deemed appropriate;
o the purpose of the account(s) and expected volume and nature of account activity;
o any immediate family members or close associates with transaction authority over the account or benefitting from transactions conducted through the account.

Should an existing Ripple Trade user be identified as a PEP, AML Compliance staff will contact the user in question to obtain a completed KYC form and will evaluate and verify, insofar as possible, through internet searches and any other means available, information concerning:

o the potential customer's background, income sources, source of funds and wealth and any other financial information deemed appropriate;
o the purpose of the account(s) and expected volume and nature of account activity;
o any immediate family members or close associates with transaction authority over the account or benefitting from transactions conducted through the account.

All identified PEPs require BSA Officer approval. As of June 2, 2015, access to Ripple Trade will not be allowed for any new users identified as PEPs until such time all requested documentation has been received, reviewed and approved by the BSA Officer. The Company will not conduct business with any new or existing PEP who does not provide, or refuses to provide, KYC and other requested information. In such circumstances, the BSA Officer will determine whether or not the filing of a SAR is warranted

Identified PEPs will be coded as such in the 'Annotations' database for reporting, tracking, and targeted transaction monitoring purposes. The Annotations database is an internal system managed by a central Ripple Labs administrator for recording additional information about Ripple user accounts that can be used for internal coding and tracking purposes.

2. Shell Companies

The term "shell company," refers to non-publicly traded corporations, limited liability companies (LLCs), and trusts that typically have no physical presence (other than a mailing address) and generate little to no independent economic value. Most shell

19

Ripple Trade, LLC
BSA/AML/OFAC Policy/Program – June 2015

companies are formed by individuals and businesses for legitimate purposes, such as to hold stock or intangible assets of another business entity or to facilitate domestic and cross-border currency and asset transfers and corporate mergers. Shell companies have become increasingly common tools for money laundering and other financial crimes, primarily because they are easy and inexpensive to form and operate.

Because shell companies can obscure company structure, ownership, and activities, Ripple Trade considers them to be higher risk entities. Shell companies that issue bearer shares are considered prohibited customer types and will be prevented from accessing Ripple Trade. When assessing the risk of shell companies, Ripple Trade considers the ownership structure, nature of the customer, the purpose of the account, settlor/beneficiary of the assets, the location of services, and other associated factors. Risks must be appropriately identified and managed in accordance with Program requirements.

Any identified and acceptable shell company users of Ripple Trade will be coded as such in the 'Annotations Database' and will be automatically subject to enhance due diligence, as described below.

3. Users named in multiple reported instances of suspicious activity

Any Ripple Trade user named as the subject of one (1) or more suspicious activity reports (SARs) filed with FinCEN will be subjected to EDD. As noted later in this Policy, instances of three (3) or more SAR filings require escalation to the Oversight Committee for retention or termination decision.

Additional factors determining consideration for risk-based EDD include, but are not limited to:

   o   transaction activity levels equivalent to USD equivalent of $100,000 total incoming or outgoing transactions;
   o   users with Ripple balances above $50,000; and
   o   geographic user location.

Enhanced Due Diligence

Ripple Trade conducts EDD on all higher-risk customers, as defined in the previous section.   This EDD will include:

   o   Negative news and internet searches;
   o   Collection and analysis of information on source of funds and/or purpose of transactions;

20

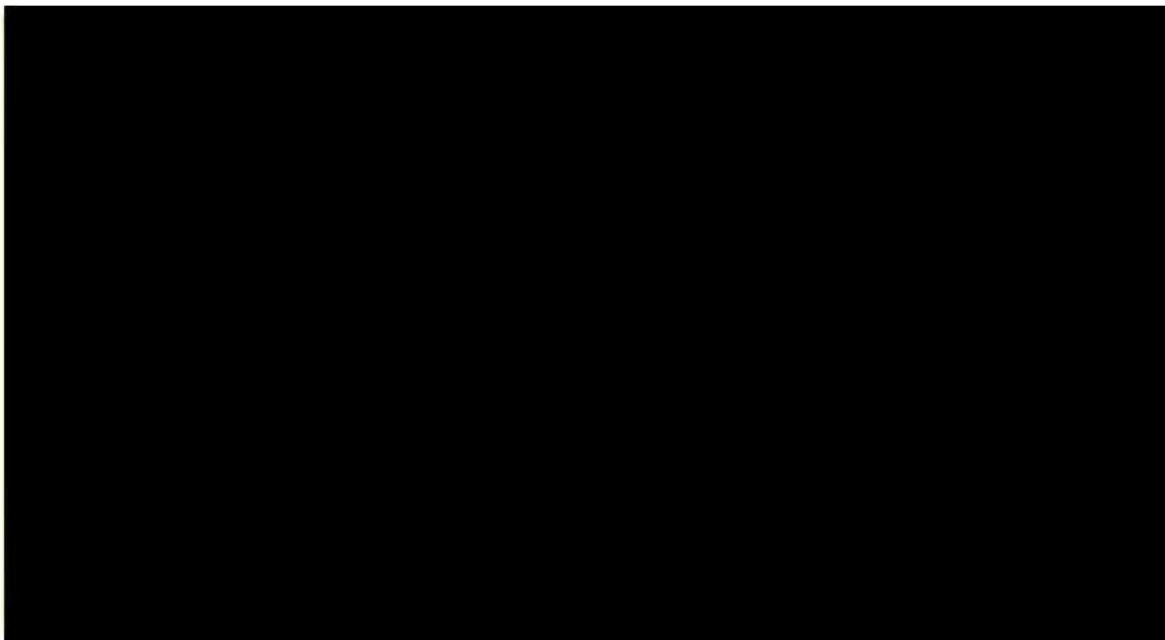Ripple Trade, LLC
BSA/AML/OFAC Policy/Program – June 2015

    o Assessment of expected transactional activity; and

    o (For existing customers) Review of actual transactional activity against expected activity and other known facts about the customer.

Ripple Trade will perform annual reviews on customers that remain above EDD transaction thresholds. In addition, the BSA Officer will close any accounts where due diligence measures cannot be applied or EDD reveals unacceptable levels of money-laundering, terrorist-financing or sanctions risks.

Monitoring Transactions for Suspicious Activity

In June 2015, Ripple Trade will implement AML transaction monitoring of activity conducted within Ripple Trade. Reports of transaction activity, including, but not limited to, reports of users with high transaction volumes, possible structured activity, dormant accounts suddenly active, transactions associated with many-to-one and one-to-many senders and receivers, will be produced monthly for review by members of the AML Compliance team to identify potential suspicious activity. The BSA Officer will, no less than annually, review the scope and calibration of transaction monitoring reports to ensure the reports are productive and aligned with identified suspicious activity.

During the user on-boarding process, and when conducting transaction monitoring, the BSA Officer, or designated staff, look for "red flags" indicators of suspicious activity. Such red flags include, but are not limited to:

21

Ripple Trade, LLC
BSA/AML/OFAC Policy/Program – June 2015
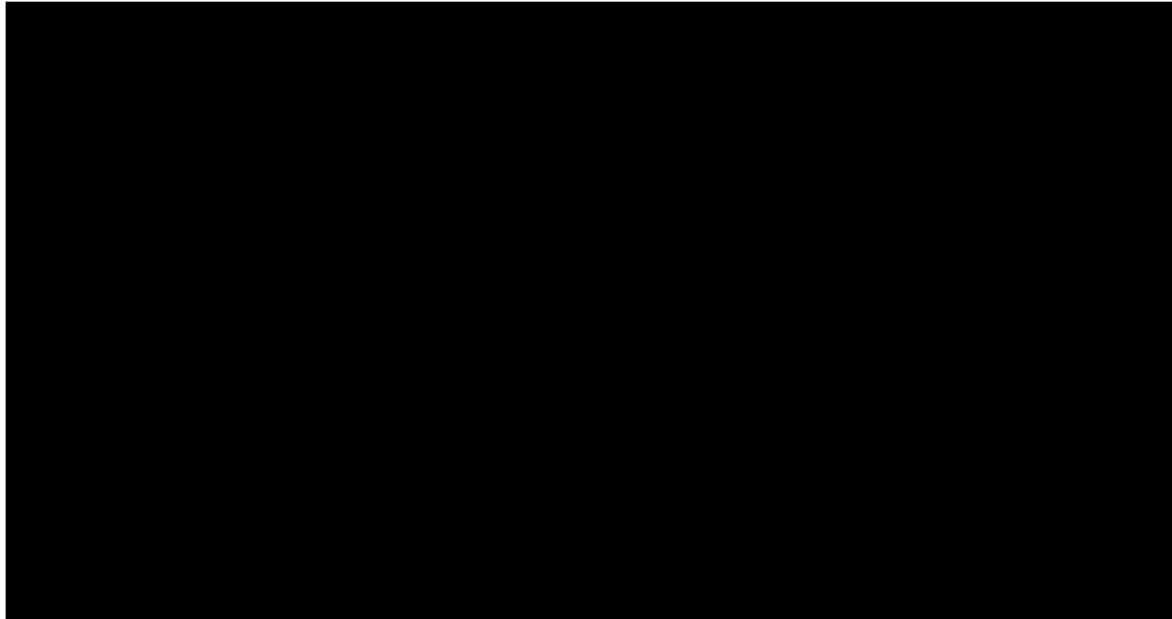
Employee Referrals of Unusual Activity

In addition to prescribed ongoing transaction monitoring conducted by AML Compliance staff, all Company employees must escalate unusual or questionable activity to the BSA Officer. Further, it is the responsibility of all Company employees to be alert to instances of unusual or questionable activity conducted by other employees, by Ripple Trade users, through the Ripple Trade Service, or unusual activity related to transactions occurring through the Company and should escalate any suspicions to AML Compliance. If an employee has reason to believe that certain activity or behavior is suspicious in nature, the employee is required to complete an Unusual Activity Report ("UAR") and submit it to the AML Compliance team for investigation and possible SAR filing. While the employee should not to attempt an investigation themselves before escalating, to the extent possible, referrals to AML Compliance should include any identifying information on the party in question, details of the related activity, information regarding additional parties to the transaction and the basis for suspecting potential illegal activity.

To facilitate internal reporting of unusual behavior or activity, the Company has established an internal Unusual Activity Reporting process governing the escalation, receipt, and processing of employee reports of unusual activity or suspected non-compliance with Ripple Trade's BSA/AML/OFAC Program. Only designated Compliance staff members have access to UARs submitted by Company employees. Reports of all incoming escalations and their ultimate resolution are maintained securely for a period of five (5) years from the date of employee submission (or from the date of SAR filing, if warranted).

22

ripple

Ripple Trade, LLC
BSA/AML/OFAC Policy/Program – June 2015

Anonymous Reporting of Unusual Activity

Should a Company employee wish to anonymously report unusual or potentially suspicious activity, or non-compliance with this BSA/AML/OFAC Program, he or she may do so using the Company's confidential reporting service, accessible via phone at ▮▮▮▮▮▮▮▮▮ or online at www.▮▮▮▮▮▮▮▮com.

Designated AML Compliance staff have direct access to the anonymous online e-mail inbox and voicemail and are responsible for maintaining strict confidentiality of reported information, disclosing only suspected activity and not the name of the individual who submitted the report, and only as necessary to implement the BSA/AML/OFAC Program. Reports of all incoming escalations and their ultimate resolution are maintained securely for a period of five (5) years from the date of employee submission.

Investigations

Ripple Trade has developed and regularly maintains detailed procedures for the investigation of alerts. All alerts from ongoing transaction monitoring efforts, or unusual or potentially fraudulent activity escalated through either internal/external activity alert channels must undergo an initial review within three business days of their escalation into AML Compliance. The initial review, which is documented, determines whether an investigation appears warranted. Should AML Compliance staff identify unusual activity during the initial review, an AML investigation will be initiated.

When warranted and to the extent possible, review of transaction activity should be expanded to assess the totality of transactions conducted by that customer and consistency of those transactions with KYC information, where available.

The AML investigator must fully document the investigation, the results, and any action taken in accordance with detailed alert review and investigation procedures. The results of all investigations are reviewed by the BSA Officer prior to investigation closure or SAR filing. Any decisions not to file a SAR following investigation must be clearly documented in the investigation file.

23

⚡ ripple

Ripple Trade, LLC
BSA/AML/OFAC Policy/Program – June 2015

Reporting Suspicious Activity

Desktop procedures for E-filing of SARs are maintained by AML Compliance. The BSA
Officer, or appointed designee, initiates SAR filing when activity involving fiat and/or
virtual currencies of different denominations and issuers greater than the equivalent of
USD $▮▮▮▮ is deemed to be suspicious in nature and any one of the following applies:
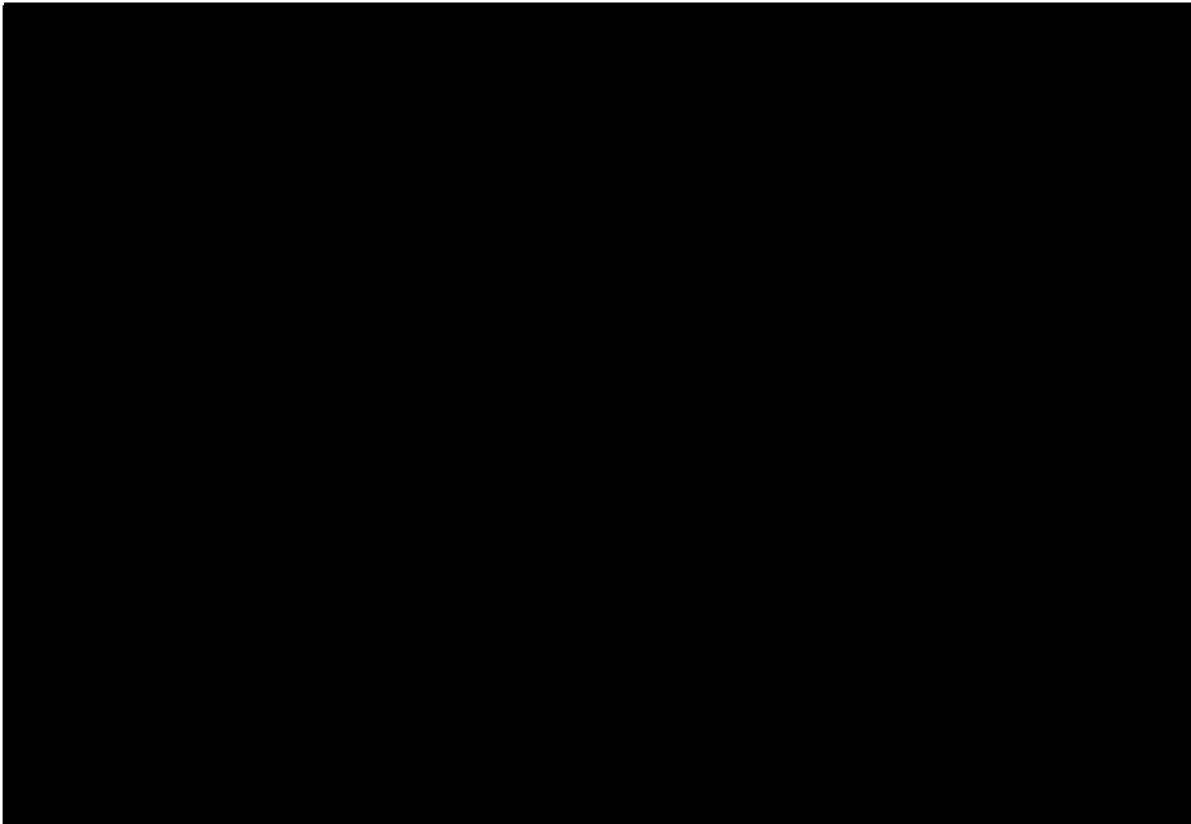
The BSA Officer may choose to report suspicious activity voluntarily if the transaction
falls below the USD $▮▮▮▮ monetary threshold in cases where a SAR may provide useful
information to law enforcement. The BSA Officer is responsible for final determination
regarding whether reporting is required or will be voluntarily made; investigation
records include the reason for the SAR/No SAR decision.

The BSA Officer is responsible for ensuring that the SAR is filed no later than 30 days (or
within 60 days if a suspect cannot be identified) after the determination that suspicious
activity has occurred.

If the BSA Officer determines that identified violations require immediate attention,
such as in the case of egregious and ongoing money laundering, she will immediately

---

[3] Potential criminal violations involving insider abuse will be reported notwithstanding the dollar amount
involved

24

Ripple Trade, LLC
BSA/AML/OFAC Policy/Program – June 2015

notify (by telephone) the appropriate law enforcement agency, in addition to filing a
SAR. Moreover, should the activity in question indicate the possibility of terrorist
activity, the BSA Officer will immediately notify the Compliance Oversight Committee
and will voluntarily report the activity to FinCEN, as appropriate.

In addition to filing a SAR, the BSA Officer will immediately notify Federal law
enforcement by telephone if:

- o The Company has reason to believe a customer is trying to move illicit funds out
  of the government's reach;
- o The Company has reason to believe a customer is about to use the funds to
  further an act of terrorism, engage in money laundering, or otherwise engage in
  illegal activity; or
- o The Company has other reasons to believe that one or more law enforcement
  agencies may benefit from direct notification of the suspicious activity.

SAR Follow-Up

In the event that a SAR is filed, the BSA Officer will determine whether user termination
is appropriate. If the user relationship is retained, the BSA Officer, or designee, will
conduct a follow-up 90-day review to determine whether reported activity has
continued and warrants the filing of an additional SAR.

All instances of three (3) SARs filed on any user relationship require automatic
escalation by the BSA Officer to the Compliance Oversight Committee for user
termination/retention decision.

Copies of SARs filed and all supporting documents must be retained securely and
confidentially for at least five (5) years from the filing date.

Maintaining SAR Confidentiality

SARs and any information which would indicate a 5AR filing, are strictly confidential. No
officer, director, employee, agent, or service provider of Company may notify any
parties that a transaction or person has been reported in a SAR.

The Company prohibits all staff from "tipping off" users that they are under
investigation or that Ripple Trade has filed a SAR naming them. The BSA Officer ensures
that all employees receive appropriate training (including the prohibition against
"tipping-off") on how to internally report unusual or suspicious activity to AML
Compliance. To reduce risk of disclosure, the Company restricts internal access to 5AR

25

ripple

RPLI_SEC 0095294

Ripple Trade, LLC
BSA/AML/OFAC Policy/Program – June 2015

filings, documentation and other SAR-related information to the BSA Officer, AML Compliance staff, and Compliance Oversight Committee members.

OFAC Compliance and Section 311 Screening

In June 2015, the Company will implement screening for existing and new Ripple Trade users, employees, vendors, service providers, and to the extent Ripple Trade can identify them, transaction counterparties of customers. Names and other identifying information (to the extent accessible to the Company) will be screened against the United States Treasury Department's Office of Foreign Assets Control ("OFAC") Specially Designated Nationals ("SDN") list and the list of countries subject to sanctions imposed by the United States ("U.S. Sanctions"), in addition to lists and jurisdictions subject to sanctions not imposed by the United States, pursuant to local sanctions laws and regulations ("non-U.S. Sanctions"), e.g., European Union ("EU") sanctions and United Nations sanctions. New and existing Ripple Trade users will also be screened against the list of Section 311 entities subject to Special Measures. Ripple Trade will not enable further transactions, or otherwise establish a relationship, with any individuals or entities subject to OFAC sanctions.

Upon implementation of the screening application any prospective new Ripple Trade user will be screened. Once Ripple Trade has obtained and verified CIP information, it will submit this through the RDC screening application. AML Compliance staff conduct initial review pursuant to Ripple Trade's detailed OFAC match verification and documentation procedures. Staff escalate any potential matches requiring further review in order to properly disposition to the BSA Officer for second-level review. No new Ripple Trade users will be on-boarded until such time as sanctions screening is complete and a 'no match' decision has been determined.

All existing Ripple Trade users are also required to undergo sanction screening upon verification of submitted CIP information. Upon identification of any potential or true OFAC matches, AML Compliance will prevent access to the Ripple Trade Service and contact any known associated Gateway to reject or freeze customer funds issued on the Ripple protocol. Ripple Trade is currently exploring the development of additional methods to 'block' Ripple Network balances funds of any identified true OFAC matched persons.

Going forward, the screening application will automatically screen all CIP-verified Ripple Trade users against updates/changes to OFAC SDN and sanctions lists and will submit results for AML Compliance review through its customized dashboard.

26

◦ ripple

Ripple Trade, LLC
BSA/AML/OFAC Policy/Program – June 2015

All true OFAC matches must be reported by the BSA Officer to OFAC, in writing, within ten (10) business days and are reported to the Compliance Oversight Committee and senior management, as identified.

The Company is in the process of implementing controls to block IP addresses from countries with broad OFAC sanctions programs, to ensure that users utilizing these IP addresses cannot establish a customer relationship with Ripple Trade or otherwise access the Ripple Trade service.

Independent Audit of the Policy and Program

The BSA Officer will identify and the Compliance Oversight Committee will approve a qualified, independent third party to conduct testing of the Company's BSA/AML/OFAC controls on at least an annual basis.

Testing will include an audit of Company's compliance with its own BSA/AML/OFAC Program and policy requirements and must include, at a minimum:

- o Evaluation of the overall integrity and effectiveness of the Program;
- o Risk-based testing of all affected areas and controls to ensure compliance with the Program;
- o A review of the most recent BSA/AML/OFAC risk assessment;
- o Reviewing the flow of funds and the scope of Company's business to determine whether additional compliance controls are needed;
- o Reviewing exception items to the BSA/AML/OFAC Program;
- o Reviewing the process for referring, investigating, and reporting unusual or suspicious activity;
- o Sampling of transaction activity for compliance;
- o Reviewing and testing compliance with recordkeeping and record retention policies;
- o Reviewing and testing procedures for customer identification and verification;
- o Reviewing and testing procedures for OFAC sanctions screening;
- o Reviewing adherence to licensing requirements and regulatory reporting obligations;
- o Evaluating the Company's response to any previously identified deficiencies; and
- o Reviewing adequacy of the Training Program.

Upon completion of the audit, the independent auditor will issue a report of findings to the Compliance Oversight Committee. The report will include any deficiencies identified and recommendations for enhanced controls, including recommended changes to the

27

ripple

Ripple Trade, LLC
BSA/AML/OFAC Policy/Program – June 2015

BSA/AML/OFAC Program and Policy, where applicable. The BSA Officer, or designee, will create and implement a comprehensive remediation plan to address each of the resulting recommendations, as appropriate, and report quarterly on remediation progress to the Compliance Oversight Committee.

Records of independent testing must be retained for at least five (5) years.

Training and Education

Ripple Trade has developed a BSA/AML/OFAC Training Program which covers new employee training, annual baseline training for employees and other covered parties (including service provider personnel whose duties impact the Program, Compliance Oversight Committee members, Ripple Labs directors and ongoing professional development for the BSA compliance team. The BSA Officer ensures that Ripple Trade personnel and any other covered parties receive appropriate BSA/AML/OFAC training.

Training includes an overview of this BSA/AML/OFAC Policy and Program, as well as a discussion of the following:

- o The Company's responsibilities for compliance under the BSA, the USA PATRIOT Act, the OFAC statutes and regulations, and any other applicable laws, including specific program controls;
- o The function of the BSA Officer and other designated roles under the BSA/AML/OFAC Program;
- o Recent changes to regulations or internal processes and controls;
- o How to identify red flags and signs of potentially suspicious activity and action to take when risks are identified;
- o Record-keeping and document retention policies; and
- o Consequences to the Company and to individuals for non-compliance, including statutory penalties and internal discipline/penalties.

New employee hires for Ripple Trade must receive initial training within 30 days of joining the Company and at least annually thereafter, or more frequently if warranted due to significant changes to regulation or the Company BSA/AML/OFAC Policy and Program.

In addition, the BSA Officer will work with Ripple Labs to establish a baseline BSA/AML/OFAC training for Ripple Labs employees not covered by the Ripple Trade Training Program whose job responsibilities may plausibly lead them to identify unusual activity involving Ripple Trade users.

28

ripple

Ripple Trade, LLC
BSA/AML/OFAC Policy/Program – June 2015

The BSA Officer, or designated AML Compliance staff, is responsible for retaining employee and covered party training attendance records and certifications for at least five (S) years from the date of training.

Correcting Program Violations

The BSA Officer will take appropriate measures to correct any violations of this BSA/AML/OFAC Program. Regarding internal violations, the BSA Officer will consult with appropriate personnel within the Company to ensure that proper corrective action is taken in accordance with applicable employment or other internal Company policy(ies).

With respect to violations of the BSA/AML/OFAC Program by external service providers, agents or subcontractors, the BSA Officer will consult with legal counsel prior to taking appropriate action in accordance with the applicable agreement with the entity.

Records of corrective action shall be retained for at least five (5) years, or longer if required by any laws implicated in the corrective action (for example, by employment or contract law).

Management Reporting

Quarterly BSA/AML Compliance Reporting

The BSA Officer will prepare quarterly reports for Compliance Oversight Committee review, which will cover (to the extent applicable):

- o   significant updates related to the BSA/AML/OFAC Program;
- o   status of efforts to remediate or enhance the BSA/AML/Program
- o   key inherent risk indicators, such as changes to transactional activity or nature of customer base;
- o   key control risk indicators, such as timeliness of EDD updates;
- o   relevant regulatory compliance and MSB updates related to virtual currency;
- o   recent relevant global money laundering enforcement actions;
- o   state regulatory reporting and licensing updates;
- o   BSA/AML examinations and audit reviews;
- o   training, compliance staffing, and technology resource needs;
- o   number of SARs filed and anonymized information about the nature of suspicious activity;

29

ripple

RPLI_SEC 0095298

Ripple Trade, LLC
BSA/AML/OFAC Policy/Program – June 2015

    o   risk assessment of any proposed new products or business endeavors; and,
    o   any other relevant regulatory reports.

Policy Variances and Exceptions

Any deviation from Program and Policy requirements must be first approved by the BSA Officer. Approval may be granted in limited circumstances and cannot be granted indefinitely. The requestor must submit a written request to the BSA Officer outlining the reason(s) for the variance, the time frame for the requested variance, and the replacement controls identified to mitigate the associated risk. The BSA Officer, or designee, is responsible for tracking, maintaining and managing, all approved Program and Policy variances, and will report these to the Compliance Oversight Committee.

Policy Administration

The BSA Officer reviews and updates the BSA/AML/OFAC Policy and Program no less than annually. The BSA Officer consults with regulatory and legal advisors, as necessary, when conducting the annual review. The Compliance Oversight Committee must review and approve updates to the BSA/AML/OFAC Policy and Program annually, or more frequently, as needed.

This BSA/AML/OFAC Policy and Program was approved by the Compliance Oversight Committee on June 12, 2015 and becomes effective as of that date.

Questions concerning this Program/Policy should be forwarded to the BSA Officer, Antoinette O'Gorman (███████@ripple.com)

30

✦ ripple

ripple trade

Ripple Trade, LLC
Compliance Oversight Committee Charter
As of June 12, 2015

Table of Contents

1.   Purpose of Committee

The Ripple Trade, LLC (known herein as "Ripple Trade" or "the Company") Compliance Oversight Committee ("the Committee") provides senior management oversight to the Company's Bank Secrecy Act/Anti-Money Laundering ("BSA/AML") and Office of Foreign Assets Control ("OFAC"; collectively, "BSA/AML/OFAC") Policy and Program ("the Program"). The Committee's primary objective is to ensure the Company complies with the BSA and all applicable money laundering and sanctions laws and regulations in all aspects of its business. The Committee achieves this objective by overseeing and implementing enhancements to the Program related to program implementation, risk assessment, and issue escalation.

2.   Membership

The Committee comprises the BSA Officer, the Ripple Labs General Counsel, and the Ripple Labs Head of Regulatory Relations and Strategic Policy Initiatives. The Chair of the Committee is the BSA Officer.

ripple

i

3.   Responsibilities

The Committee provides management-level supervision over the implementation of the Program. The Committee's responsibilities include:
- Promoting and implementing a strong culture of compliance;
- Ensuring that the Company appoints a suitably qualified BSA Officer with appropriate levels of staffing support;
- Overseeing the BSA Officer (the BSA Officer will recuse himself or herself from this responsibility);
- Regularly consulting with regulatory advisors and legal counsel to ensure that the Program remains current with applicable laws and leading industry standards;
- No less than annually, approving the Program, the BSA/AML/OFAC risk assessment and the BSA/AML/OFAC Training Program;
- Establishing and communicating an appropriate risk tolerance for BSA/AML/OFAC risk;
- Reviewing compliance reports and any compliance issues escalated to executive management, including mitigation plans;
- Periodically reviewing the adequacy of compliance resources through the Company's BSA/AML/OFAC risk assessment;
- Reviewing periodic BSA/AML/OFAC compliance reports from the BSA Officer;
- Approving a qualified, independent third party to conduct testing of the Company's BSA/AML/OFAC controls on at least an annual basis;
- Reviewing the results of independent testing and examinations, ensuring that Ripple Trade takes appropriate action to remediate or enhance its Program taken, where indicated; and
- Reviewing and approving the Implementation Plan, which includes all specified Settlement Agreement actions as well as items necessary to fully implement Ripple Trade's Program.

4.   Reporting

The BSA Officer provides the following reporting to the Committee:
- Quarterly reporting evidencing appropriate governance of the Program;
- Any material issues of BSA/AML/OFAC non-compliance and the BSA Officer's corrective action response;
- Suspicious activity trends, including all instances of three (3) or more SAR filings on the same customer; and
- All approved Program variances.

ripple

2

The BSA Officer and/or the Committee will periodically report the following to the Ripple Labs Board of Directors:

- The Committee's approval of each risk assessment; and
- Validation reporting evidencing appropriate governance of the Program on a semi-annual basis.

5.   Meetings

The Committee meets at least quarterly or more frequently as needed. The Committee Chair may invite additional persons to Committee meetings as necessary for the Committee to carry out its responsibilities effectively.

6.   Committee Charter Administration

At least annually, the BSA Officer reviews this Charter, and recommends any appropriate changes for review and approval by the Committee. The review includes consideration of applicable law, feedback on the effectiveness of the Committee, and any supervisory or audit input. The next targeted revision date of this Charter is June 10, 2016.

REVISION DATE	CHANGE	APPROVAL DATE
n/a	New Committee Charter	June 12, 2015

ripple

3

Ripple Trade, LLC
BSA/AML/OFAC Training and Education Program
June 2015

Training and Education Program Overview

Ripple Trade, LLC ("Ripple Trade" or "the Company"), its executive management, and its parent company's (Ripple Labs) Board of Directors are committed to ensuring that its products and services are not used to launder money, finance terrorism, evade U.S. Government sanctions or otherwise facilitate criminal activity. The Company's BSA/AML/OFAC Policy and Program sets forth Ripple Trade's controls and compliance obligations with regard to Anti Money Laundering ("BSA/AML") and Sanctions rules and regulations.

The following BSA/AML/OFAC Training and Education Program describes Ripple Trade's required training for employees and any other covered parties (including service provider personnel whose duties impact the Program, Compliance Oversight Committee members, and Ripple Labs directors) to ensure that sufficient training to comply with the provisions of BSA/AML and Sanctions rules and regulations in the course of his or her job function. In addition to annual BSA/AML/OFAC training which all Ripple Trade employees must complete, Ripple Trade AML Compliance staff also attend additional internal and/or external training sessions, conferences and continuing education programs to remain current with AML and sanctions compliance requirements. The BSA Officer will also provide annual training to employees of Ripple Labs not covered by the Ripple Trade Training Program whose job responsibilities may plausibly lead them to identify unusual activity involving Ripple Trade users.

Roles and responsibilities

It is the responsibility of the BSA Officer to ensure that this Training and Education Program is immediately implemented. The BSA Officer is also responsible for informing senior management of any employees who do not appropriately follow the Company's BSA/AML/OFAC policy and/or fails to complete his or her training obligations in accordance with this Program. The status of Ripple Trade employee BSA/AML/OFAC training is also reported by the CCO/BSA Officer to the Compliance Oversight Committee on a quarterly basis.

A designated Compliance Analyst is responsible for documentation and record-keeping of attendance at internal BSA/AML/OFAC training sessions as well as recording of AML training certifications and any external BSA/AML/OFAC education and training sessions. All records are maintained in the 'Training' folder, within the Ripple Trade AML Program files located on the Compliance designated secure server for a period of five years following the date of training or as specified in Ripple Trade's Record Retention Policy.

l

rippleLabs

Ripple Trade, LLC
BSA/AML/OFAC Training and Education Program
June 2015

The file location of Ripple Trade's training folder is:
rnc / Ripple Trade AML / OFAC Program / 7-AML Training Program / 2015 / Final
The Record Retention policy is located at:
rnc / Ripple Trade AML / OFAC Program / 3-AML Procedures

Schedule

All Ripple Trade employees and any other covered parties are required to undergo annual BSA/AML/OFAC training. Any new Ripple Trade employees and other covered parties will be required to undergo BSA/AML/OFAC training within thirty days of hire date.

Ripple Trade's Compliance Oversight Committee members as well as members of Ripple Labs' Board of Directors are also required to undergo annual training conducted by the Chief Compliance Officer.

It is the objective of the Company that as many Ripple Trade AML Compliance employees as possible are CAMS (Certified Anti Money-Laundering Specialist) certified and receive ongoing BSA/AML/OFAC training opportunities. All AML Compliance employees are encouraged to attend external training events and webinars relevant to BSA/AML/OFAC compliance.

A tracking sheet of training sessions attended in 2015 to date is attached as **Exhibit B** to this document.

Annual Training

All Ripple Trade employees and other covered parties, as applicable, are required to attend BSA/AML/OFAC training on an annual basis or more frequently, if warranted. Ripple Trade's annual training covers:

- Company compliance responsibilities under the Bank Secrecy Act (BSA), the USA PATRIOT Act, Office of Foreign Assets Control ("OFAC" or, more broadly, "sanctions") regulations, and any other applicable AML laws;
- Specific Ripple Trade AML/OFAC program controls;
- Designated roles in the AML/OFAC Program

2

rippleLabs

Ripple Trade, LLC
BSA/AML/OFAC Training and Education Program
June 2015

- The function of the CCO/BSA Officer;
- Any recent changes to regulations and/or internal processes and controls;
- How to identify 'red flags' and indications of unusual activity and specific action to take when AML risks are identified;
- The Company's record-keeping and document retention policies; and
- Consequences to the Company and to Ripple Trade employees for non-compliance with AML/OFAC Program requirements, including statutory penalties and internal discipline/penalties.

The June 2015 BSA/AML/OFAC Training presentation can be found here:
rnc / Ripple Trade AML / OFAC Program / 7-AML Training Program / 2015 / Final

Attendance records and certifications for the training held in June 2015 is located here:
rnc / Ripple Trade AML / OFAC Program / 7-AML Training Program / 2015 / Final

Supplementary Training

In addition to annual BSA/AML/OFAC training, Ripple Trade AML Compliance staff, including the BSA Officer, must attend a minimum of ten (10) hours of internal or external Payments and/or AML-related education and training sessions. Attendance records at these sessions is documented and logged on an internal tracking list maintained by AML Compliance and saved in the Ripple Trade AML Training Program folder located here:
rnc / Ripple Trade AML / OFAC Program / 7-AML Training Program / 2015 / Final

BSA/AML/OFAC training records along with a roadmap for AML Compliance continuing education are tracked and documented by the AML Compliance team. A tracking sheet of training sessions attended throughout the year is attached as **Exhibit A** to this document.
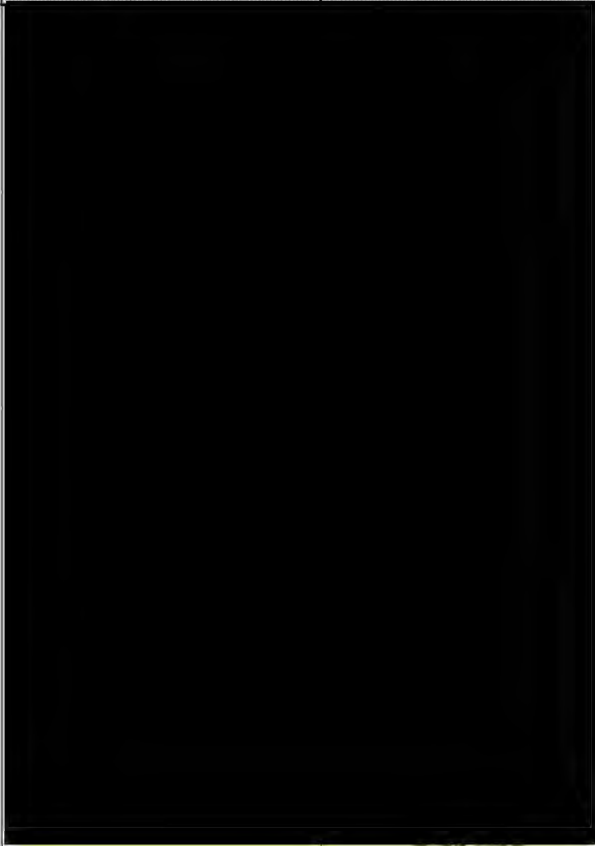
A tracking sheet of training sessions attended by Compliance Personnel in 2015 to date is attached as **Exhibit B** to this document.

3

&**ripple**Labs

Ripple Trade, LLC
BSA/AML/OFAC Training and Education Program
June 2015

Exhibit A[1]: Annual AML Compliance Training for Ripple Trade Employees

Date	Training Type	Presenter	Present	Hours
6/8/2015 – 6-16-15	Annual AML Training	███████████	███████████	1

---

[1] Note: Additional annual AML training will be scheduled in the latter part of 2015 for remaining Ripple Labs employees and for Ripple Labs Board of Director members

4

rippleLabs

Ripple Trade, LLC
BSA/AML/OFAC Training and Education Program
June 2015

Exhibit B: 2015 AML Compliance Training and Education Tracking List

Date	Regulation/Opinion	Presenter	Present	Hours
02.17.2015	Internal discussion on Draft EU Proposed AML Directive issued December 2014			1.5
02.23.2015	Global Monitoring Tool overview and training			1
02.26.2015	ACAMS Model and Validation Tuning			2
03.11.2015	Payments Training			2
03.15.2015	CAMS certification test prep, ACAMS, Florida			8
04.01.2015	Webinar: Lessons Learned From Recent Virtual Currency Cases			2
05.06.2015	Webinar: Effective SAR filing			2
05.21.2015	CAMS Certification Exam			N/A
06.01.2015	CAMS Certification Exam			N/A

5

rippleLabs

Ripple Trade, LLC

Monitoring/Investigations/SAR Guidelines

June 2015

Table of Contents

rippleLabs

Ripple Trade, LLC
Monitoring/Investigations/SAR Guidelines
June 2015

Overview:

The primary task of Ripple Trade's Compliance Monitoring and Investigations team is to serve as the centralized function for detection, prevention and reporting of potentially suspicious client activity, money laundering or terrorist financing. The Compliance Monitoring and Investigations team reports directly to the BSA Officer.

Objectives:

The Company's BSA/AML/OFAC Program and Policy requirements include effective monitoring to assist with prevention and detection of possible money laundering, terrorist financing, or other types of unlawful activity, investigation of identified activity and reporting all suspicious activity identified to the Financial Crimes Enforcement Network ("FinCEN"). To facilitate this, under the direction of the BSA Officer, Compliance Investigations Analysts maintain responsibility for:

1. developing and maintaining investigations systems processes; and
2. effective supervision of AML and terrorist prevention efforts for Ripple Trade.

MONITORING

Transaction Monitoring Review:

At a minimum, the following information should be available/obtained to assist during the transaction monitoring review process, if applicable:

1) Excel spreadsheet of alerted transactions;
2) Open-source internet searches (Google, Yahoo, etc.) on the alerted Ripple user and counterparties;
3) Negative news searches (on all identified parties);
4) User KYC and CIP information obtained prior to account opening (for new Ripple Trade users) or obtained following the June 2015 launch of Company's new CIP process to capture and verify and record required CIP and KYC information (where needed) for existing Ripple Trade

rippleLabs

2

Ripple Trade, LLC
Monitoring/Investigations/SAR Guidelines
June 2015

users. Under the terms of a recent Settlement Agreement with regulators[1], an initial grace period (until October 30, 2015) is allowed for submission and verification of CIP information for existing Ripple Trade users. After this time, if user CIP information is not submitted, or cannot be appropriately verified through automated or manual means, user access to Ripple Trade will be disabled; and

5) Transaction activity details (expected and historic transactions)

1) The Analyst reviews underlying alert triggering information and notes the alert referral source (e.g., internal employee notifications submitted via an Unusual Activity Report ("UAR" – file locations identified directly below), ongoing transaction monitoring parameters, external alerts, etc.)

   Paths to file:

   Unusual Activity Report (UAR) form:
   https://docs.google.com/a/ripple.com/forms/ ███████████████████████
   ██████████████

   Unusual Activity Report, Employee Internal Alert Procedures:
   https://docs.google.com/a/ripple.com/document ███████████████████████
   ███████████████

   Link to External Alert Workflow Process for Ripple Labs User Support and AML Compliance:
   https://docs.google.com/a/ripple.com ████████████████████████
   ██████████████

2) Analyst identifies all accounts associated with the alert. This can be done by entering the account in the internal Risk Tools ████████████████

3) Analyst identifies if focus is a higher-risk individual or entity. Examples of higher-risk individuals or entities are:

   ██
   ██
   ██
   ██
   ██

---

[1] In May 2015 Ripple Labs and its wholly owned subsidiary XRP II entered into a Settlement Agreement with the Department of Justice and FinCEN.

rippleLabs

3

Ripple Trade, LLC

Monitoring/Investigations/SAR Guidelines

June 2015

INVESTIGATIONS

How to Conduct an Investigation

Ripple Labs has designed and developed a proprietary risk monitoring and analytical tool that enables protocol-wide transaction activity monitoring and analysis. In addition to capturing all transaction activity on the Ripple protocol, recent enhancements include the addition of structured transaction threshold parameters, identification of transaction counterparties, degrees of separation and flow of funds reporting. These capabilities are further described below:

rippleLabs

4

Ripple Trade, LLC

Monitoring/Investigations/SAR Guidelines

June 2015
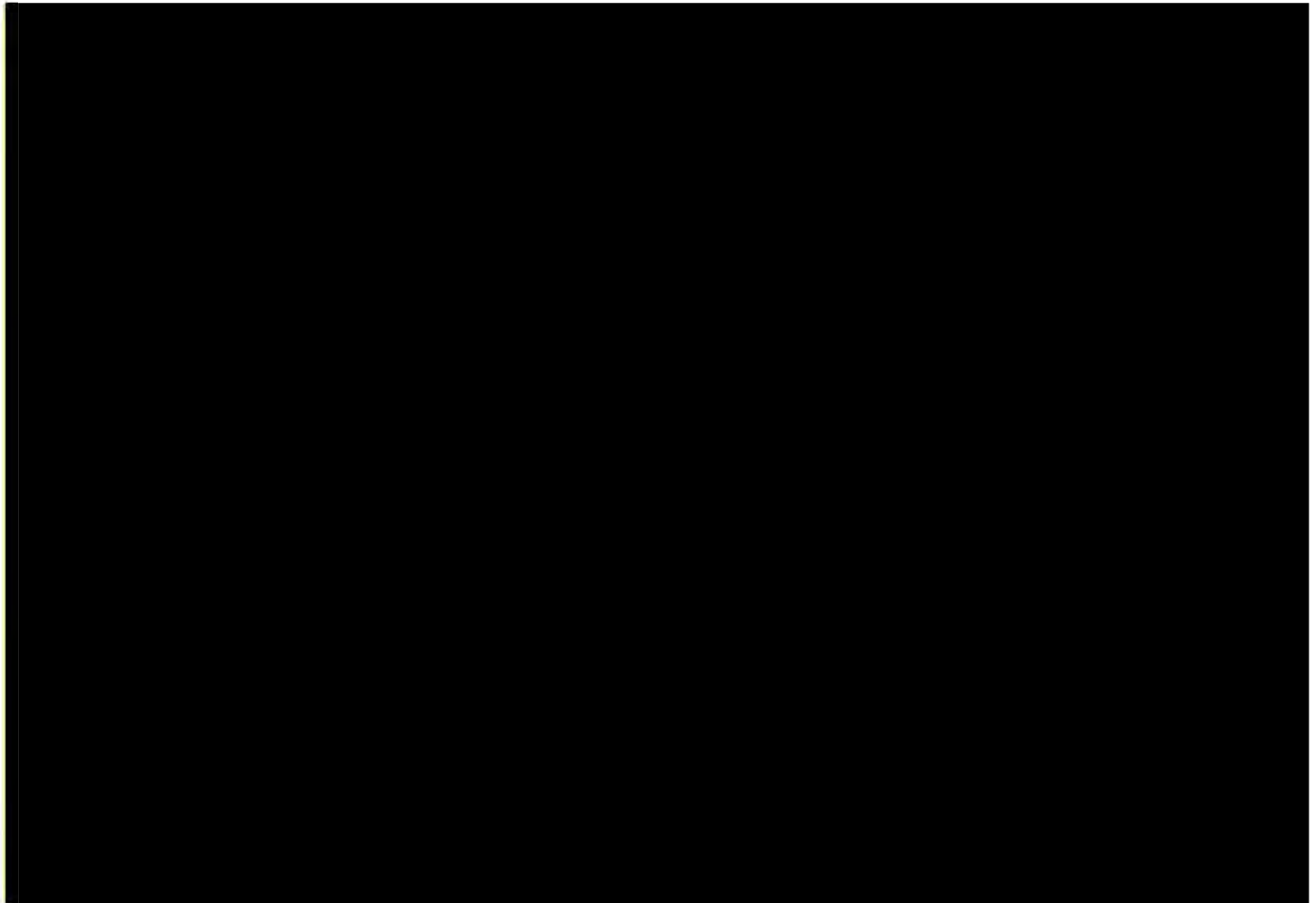
Transaction Review:

Analyst begins the transaction review process by comparing alerted Ripple Trade activity against the user's transaction history and to the expected activity documented on the user's KYC profile, where available, to determine if the alerted activity falls within the user's expected pattern of behavior (note: this information will be available for higher risk users and non-individual Ripple Trade users following implementation of the new CIP process scheduled for launch in late June 2015; until CIP has been obtained and verified, Ripple Trade will have little to no user information available to use during investigation into unusual activity.)

In situations involving alerted transactions and including large numbers of counterparties, the Analyst reviews a minimum of eight (8) counterparties (per Ripple Trade user wallet) taking into consideration the following:

rippleLabs

5

Ripple Trade, LLC

Monitoring/Investigations/SAR Guidelines

June 2015
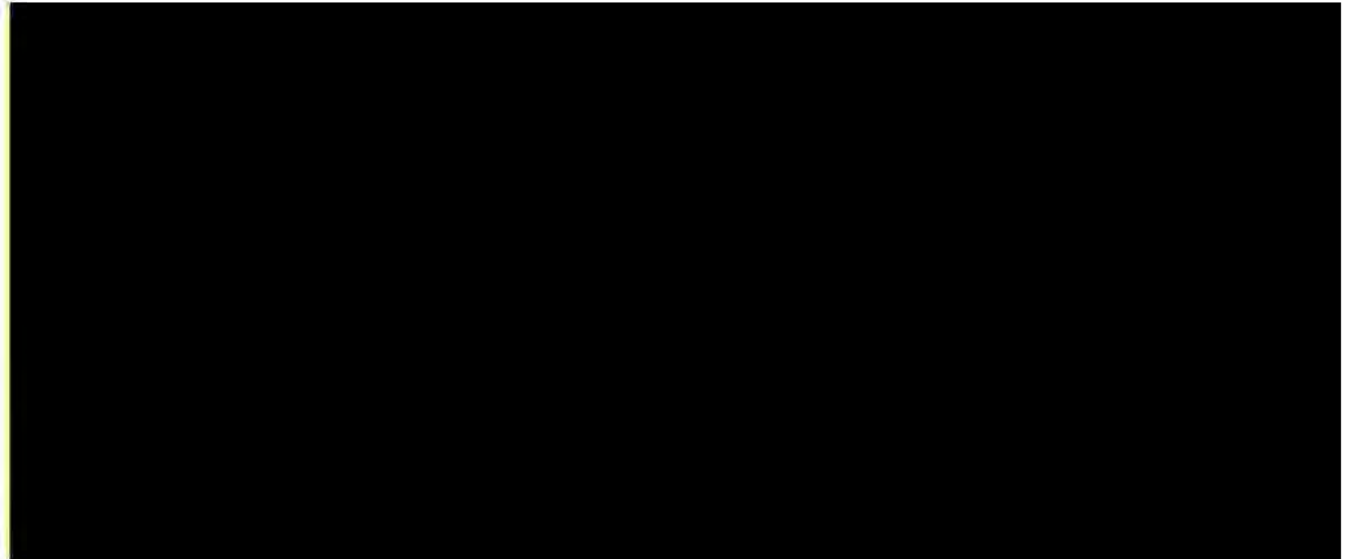
Analyst concludes the review by analyzing the above information and documenting the investigative findings in support of the Analyst's disposition. The Analyst attaches all supporting documentation obtained during the review (supporting documentation refers to all documents or records that assisted in making a decision about the nature of the activity under review.) Once the Analyst determines whether or not the activity is suspicious, a written recommendation is prepared. The disposition synopsis must be clear and concise containing only the information necessary to substantiate the decision reached and should address the following elements: who, what, when, where, why, and how. A factual description of the activity reviewed, the reason(s) why the activity does, or does not, appear to warrant additional investigation, and relevant supporting information must be included along with the Analyst's review disposition.

Available recommendations include: (1) Alert cleared; or, (2) Alert escalated. If the decision is made to clear the alert, the Analyst provides an explanation as to why the activity does not appear to be unusual.

In some cases, additional information may be required from the user. Depending on the nature of the issue, the Analyst should brief the BSA Officer and follow her direction. The Analyst will contact the user directly to inquire about the questioned user activity in question.

AML INVESTIGATIONS

At a minimum, for Ripple Trade investigations, the scope of the transaction review should encompass transactions conducted in the prior three month period. Further expansion of review scope is at the

Ripple Trade, LLC

Monitoring/Investigations/SAR Guidelines

June 2015

Analyst's discretion. For investigations which do not have a defined scope of review (ad hoc, etc.), the cases are escalated to the BSA Officer for determination.

The Analyst reviews activity sufficient to understand the overall nature of the activity and should search the case management system to determine if there are any prior investigations that should also be considered.

If the activity cannot be explained after the initial scope of review, the Analyst may conduct an additional account review in 30-day increments. Continued expansion of scope is not required if no further activity is identified.

QA Reviews of Completed Investigations:
Once the Analyst has completed an investigation and drafted a recommendation, the case is forwarded to the BSA Officer for review and approval. If the Analyst determines that a SAR is not warranted, the reason and supporting documentation should also be documented fully and presented for BSA Officer review.

Escalations of Significant Activity
Escalation to Compliance Oversight Committee is required for cases involving user accounts where reputational or other significant AML risk is identified. The following matters must be escalated by the BSA Officer to the Oversight Committee:

Once an investigation is complete, the Compliance Investigations Analyst can flag any 'blacklisted' user accounts in the internal Annotation database for future tracking purposes. Accounts are also be 'blacklisted' following review of activity reported by other users or gateways of alleged fraudulent or other illegal activity within Ripple Trade, by a Ripple Trade, or otherwise associated with a Ripple Trade user.

rippleLabs

7

RPLI_SEC 0095314

Ripple Trade, LLC

Monitoring/Investigations/SAR Guidelines

June 2015

SUSPICIOUS ACTIVITY REPORTS (SARs):

The purpose of the SAR is to provide appropriate law enforcement authorities with complete and accurate information relating to known or suspected criminal activities or violations of the law observed by Ripple Trade.

Reporting Suspicious Activity

The BSA Officer, or appointed designee, will file a SAR if the amount of suspicious activity identified is over USD $█████ and:
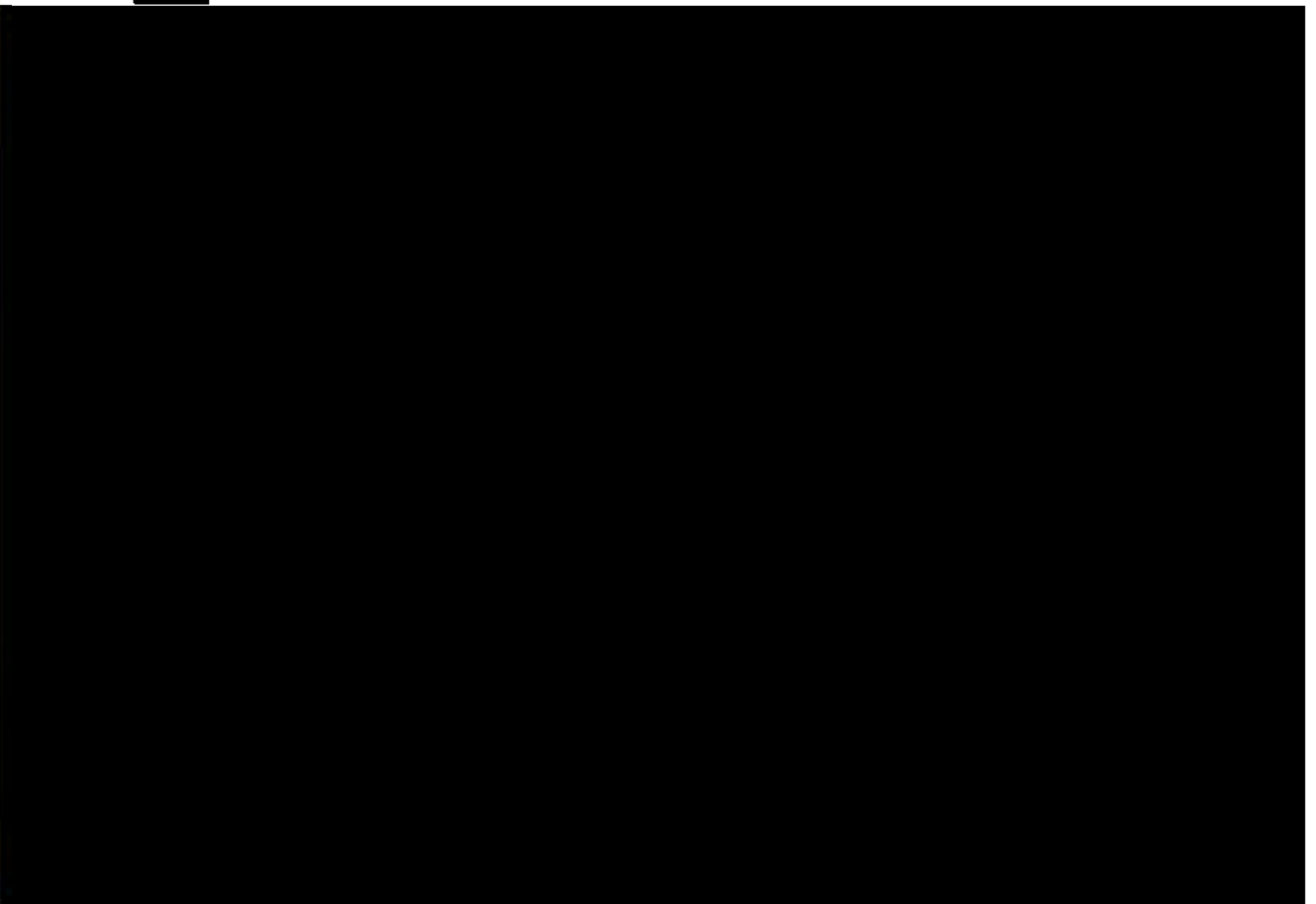
The BSA Officer may choose to report the suspicious activity voluntarily if the transaction falls below the USD $█████ monetary threshold in cases where a SAR may provide useful information to law enforcement. The BSA Officer is responsible for the final determination regarding whether a report is required or will be voluntarily made.

rippleLabs

8

RPLI_SEC 0095315

Ripple Trade, LLC
Monitoring/Investigations/SAR Guidelines
June 2015

The information generated from SAR filings plays an important role in identifying potential illegal activities such as money laundering and terrorist financing, and assists law enforcement in detecting and preventing the flow of illicit funds through our financial system. Therefore, the SAR form should include specifics on the following:

Who is conducting the suspicious activity?
While one section of the SAR form calls for specific suspect information, the narrative should be used to further describe the suspect or suspects, if known and any other information and identification numbers associated with the suspects.

When did the suspicious activity take place?
If the activity takes place over a period of time, indicate the date when the suspicious activity was first noticed and describe the duration of the activity. When possible, in order to better track the flow of funds, individual dates and amounts of transactions should be included in the narrative rather than only the aggregated amount.

Where did the suspicious activity take place?
The narrative should indicate where the suspicious activity took place (within Ripple Trade, associated with a Ripple Trade user, etc.) The narrative should also indicate, where available, associated geographic jurisdictions.

Why does the activity appear to be suspicious?
The SAR must describe, as completely as possible, why the activity or transaction is considered suspicious for the Ripple Trade user or associate party.

How did the suspicious activity occur?
The narrative should describe the "modus operandi" or the method of operation of the subject conducting the suspicious activity. In a concise, accurate, and logical manner, the narrative should describe how the suspect transaction or pattern of transactions was committed. For example, if what appears to be structuring of transactions is matched with outgoing funds transfers from user account(s), the SAR narrative should include information about both the structuring and outbound transfers (including dates, destinations, amounts/currencies, accounts, frequency, and beneficiaries of the funds transfers, where known.)

FinCEN has issued guidance on the inclusion of several key terms in the SAR narrative. The use of these key identifiers within the SAR assists law enforcement in identifying trends in criminal activity. Here is the link to the FinCEN guidance: http://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2012-G002.pdf

rippleLabs

9

RPLI_SEC 0095316

Ripple Trade, LLC

Monitoring/Investigations/SAR Guidelines

June 2015

SAR Filing Governance, Roles and Responsibilities:
It is the responsibility of the BSA Officer to review and ensure proper implementation of these procedures. The designated AML Compliance Analyst is responsible for adhering to these procedures, for filing SARs on suspicious activity via FinCEN's eFiling website and for maintaining and updating (subject to BSA Officer approval) the SAR investigation and SAR filing procedures.

Ripple Trade's e-filing account is registered under Antoinette O'Gorman, Ripple Trade's BSA Officer.

Procedures for E-Filing via FinCEN's BSA E-Filing website:
See "/rnc/Ripple Trade AML OFAC Program/3-AML Procedures/ 2015/BSA E-filing Procedures/ Final Document/ "BSA E-filing Procedures" for BSA E-Filing Procedures

SAR Timing:
SAR rules require that a SAR be filed no later than <u>30 calendar days from the date of the initial detection of the suspicious activity, unless no suspect can be identified, in which case, the time period for filing a SAR is extended to 60 days.</u>

SARs may also be filed for continuing activity that occurred within 90 days of the last SAR filing date. Follow-up SARs must be filed <u>prior to</u> the 120th day from the previous SAR file date. Ripple Trade may file a supplemental SAR on continuing activity earlier than the 120-day deadline if it believes the activity warrants earlier review by law enforcement.
(Ref: http://www.fincen.gov/forms/files/FinCEN%20SAR%20ElectronicFilingInstructions-%20Stand%20Alone%20doc.pdf)

SAR Confidentiality:
Under U.S. law, it is a crime to disclose to any person involved in the activity reported in a SAR that the activity has been reported. No Ripple Trade employee or person associated with Ripple Trade may tell, suggest, or 'tip off' a user or any person outside of Ripple Trade who may have been involved in a transaction for which a SAR was filed or will be filed.

SARs, investigations, and related information are highly sensitive and confidential. This information may be shared on a need-to-know basis only. If information is shared, care is to be taken to underscore that the information may not be further shared except as directed by the BSA Officer and/or Legal Counsel. Moreover, the fact that the activity is being or has been reported to government authorities must not be disclosed to any person that is involved in the activity.
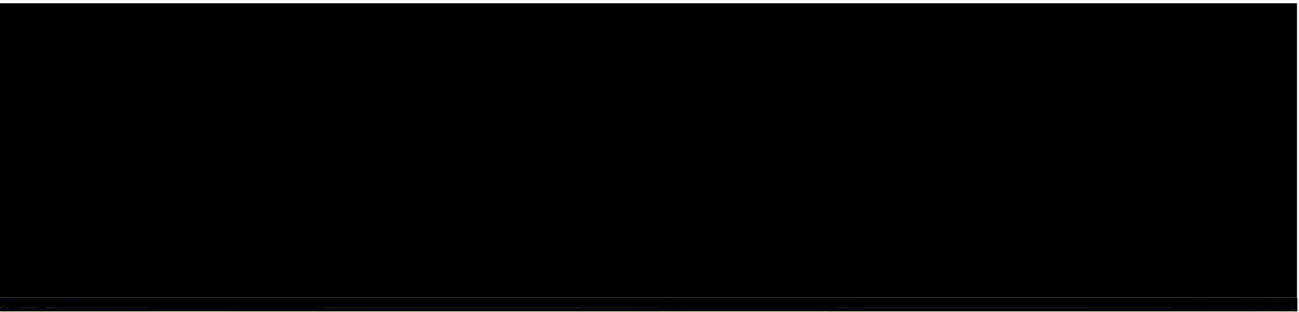
rippleLabs

10

Ripple Trade, LLC

Monitoring/Investigations/SAR Guidelines

June 2015

Person(s) Responsible for SAR Filing:
A designated member of the AML Compliance team is responsible for the completion and filing of approved (by the BSA Officer) SARs with FinCEN.

Multiple SARs:

SAR Reporting:
At least quarterly, the BSA Officer shall include data in the BSA Compliance report to the Oversight Committee relating to SAR reporting. SAR reporting data includes information on Ripple Trade users subject of multiple SARs; SARs involving employees; and/or SARs determined to present elevated reputation risk due to law enforcement interest, or indication of possible patterns of activity impacting Ripple Trade.

SAR Amendments:
AML Compliance will file an amended SAR if an error is subsequently identified after the SAR is filed, or if Ripple Trade obtains additional information pertinent to the investigation that was unavailable at the time of initial filing. An amended SAR may also be filed if the activity under review occurred before the date range of the prior SAR but was not reported in the prior SAR.

PENALTIES FOR NON-COMPLIANCE
The Company and company employees may face civil and criminal penalties for failing to properly file SARs, including, but not limited to, any combination of fines, regulatory restrictions, or imprisonment.

DOCUMENTATION RETENTION AND RECORD-KEEPING
The AML Compliance Analyst retains all SAR files and supporting documents related to SARs, alerts, and cases for a minimum period of five years after the filing or item date. Additionally, the Company will

rippleLabs

11

Ripple Trade, LLC

Monitoring/Investigations/SAR Guidelines

June 2015

provide all documentation supporting the filing of a SAR upon request to FinCEN or an appropriate law enforcement or regulatory agency. Supporting documentation refers to all documents or records that assisted the Compliance Analyst in making a decision about the nature of the user and/or activity under review. No legal process is required for the disclosure of supporting documentation to FinCEN or an appropriate law enforcement or regulatory agency.

All investigations and SAR-related documentation is saved by the Compliance Analyst to the Compliance Analyst's secured server RNC Compliance folder and subfolder: **rns/SARs/RippleTrade**

In addition to filing SARs, the BSA Officer notifies law enforcement of cases that may be of particular interest to specific agencies. The Company also responds as appropriate to requests for information from FinCEN and other governmental entities, and, when appropriate, undertakes voluntary information sharing as provided in 31 C.F.R. § 314(b).

GRAND JURY / LAW ENFORCEMENT SUBPOENAS

Upon receipt of a Law Enforcement Subpoena, the BSA Officer initiates an internal investigation into any parties/accounts referenced in the document. As the investigation progresses, it may be expanded to include other parties and accounts. The designated AML Compliance Analyst also performs a transaction review for the scope of review identified in the subpoena. A relationship analysis must be performed for all cases involving a grand jury or law enforcement subpoena on a dormant account.   The Company's law enforcement response procedures are outlined and located on the Compliance Department's secure drive: **/rnc/Law Enforcement Requests/ "Law Enforcement Subpoena Requests"**

** rippleLabs**

12

Ripple Trade, LLC

Monitoring/Investigations/SAR Guidelines
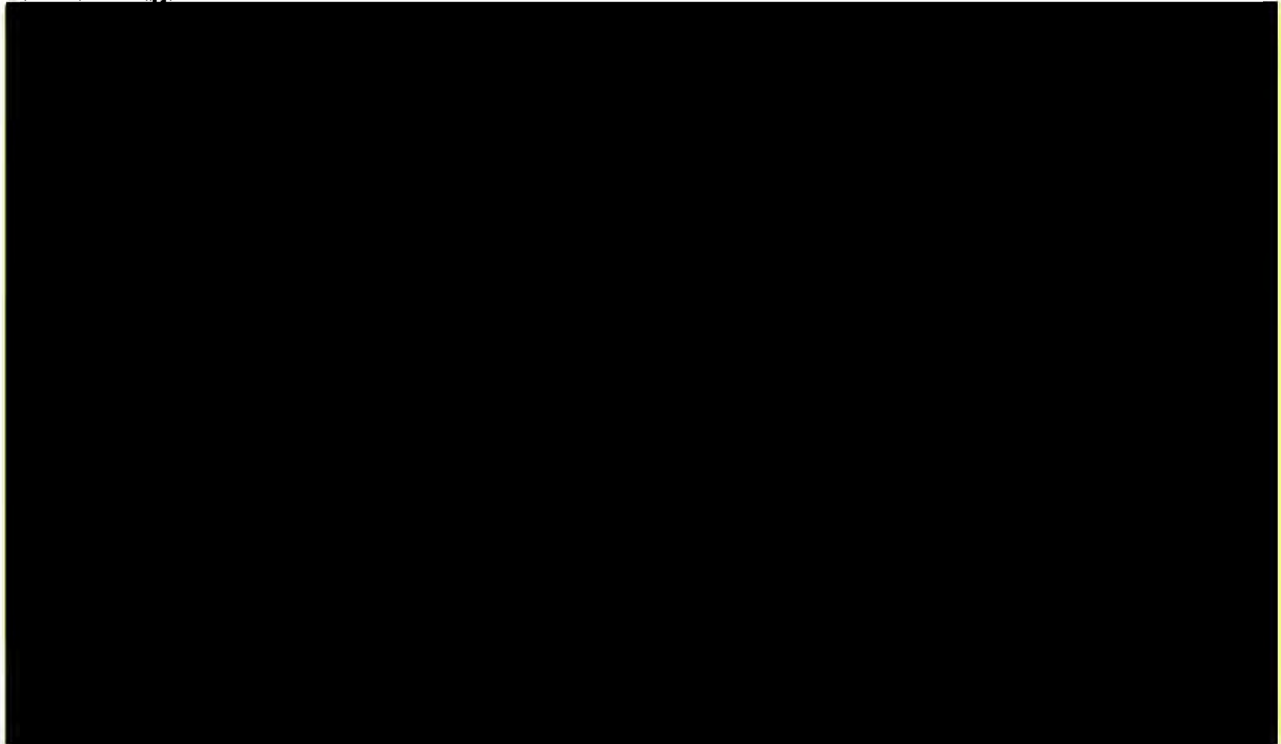
June 2015

Appendix

RED FLAGS FOR MONEY-LAUNDERING

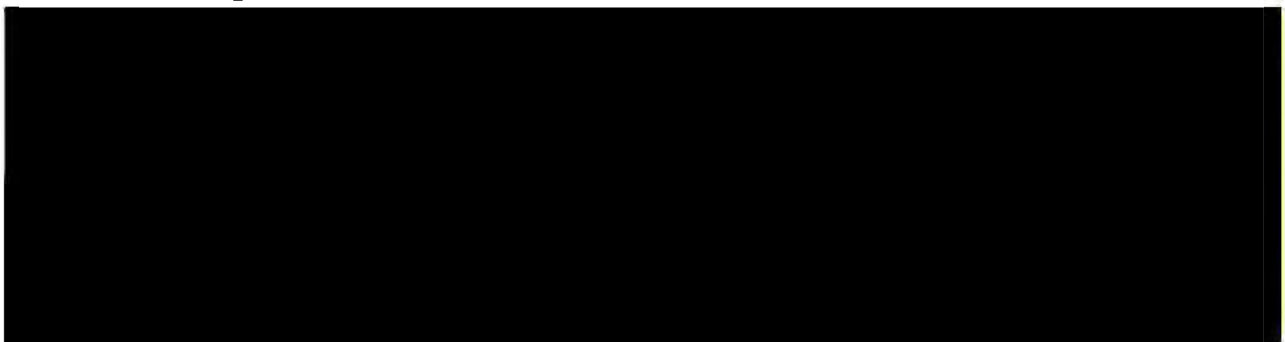**Examples of red flags include, but are not limited to, the following:**

General Examples:

User Red Flags:

Transaction Red Flags:

RippleLabs

13

XRP II, LLC
BSA/AML/OFAC Policy 2015

TABLE OF CONTENTS

ripple

l

XRP II, LLC
BSA/AML/OFAC Policy 2015

INTRODUCTION

XRP II LLC (formerly "Fund II LLC," "XRP II" or the "Company") is committed to ensuring that its products and services are not used to launder money, finance terrorism, evade US government sanctions or otherwise facilitate criminal activity. It is the policy of the company to comply fully and continuously with Anti-Money Laundering ("BSA / AML") legislation, its implementing regulations and guidance. This Policy outlines XRP II's efforts to detect and deter money laundering and terrorist financing, and provides an overview of the major functions and responsibilities within the Company's BSA/AML/OFAC Program.

XRP II engages in the sale and transfer of the virtual currency XRP to various third parties on a wholesale basis. XRP II makes these sales of XRP for the benefit of Ripple Labs, its ultimate parent company. Ripple Labs created and maintains the Ripple protocol, an open source, peer-to-peer payment protocol that enables free instant payments in any currency. XRP II's sales of XRP represents one method by which Ripple Labs raises working capital. XRP II has no other products or services and currently has no intention to develop any. If this changes in future, the Head of BSA/AML will update both the risk assessment and this document, as well as implementing any new or enhanced controls necessary, prior to the Company launching the new product or service.

SCOPE

Scope and Applicability:

The Policy applies to all XRP II business activities. All XRP II personnel are subject to the BSA/AML/OFAC Policy.

The Company recognizes that noncompliance can expose us to substantial risk and civil or criminal penalties. All employees are responsible for understanding this Policy/Program and undertaking any specific responsibilities assigned to them.

Non-compliance with, or violation of, the Policy/Program's requirements by employees may result in:
- **Disciplinary action, including termination in appropriate cases; and/or**
- **Civil and/or criminal penalties.-**

Willful blindness, or "turning a blind eye," to a potential money laundering violation can expose both the Company and individuals to potential liability.

DESIGNATION OF BSA/AML OFFICER

The Company has designated a BSA/AML Officer (Head of BSA/AML) in support of the Chief Compliance Officer, to direct, implement, enforce, maintain, and update the Company BSA/AML/OFAC Policy and Program.

2

XRP II, LLC
BSA/AML/OFAC Policy 2015

The Head of BSA/AML reports directly to the Chief Compliance Officer. She and her employees have the authority to access all company records and direct all company personnel as necessary to implement this Policy and Program.

ROLES AND RESPONSIBILITIES

All levels of XRP II management and staff carry out key BSA/AML/OFAC compliance risk management functions. These risk management functions work together to form a comprehensive system of BSA/AML/OFAC compliance risk management.

Below is a brief description of the roles and responsibilities of the various functions of XRP II with respect to BSA/AML/OFAC compliance.

BSA/AML Officer

XRP II's Head of BSA/AML, in support of the Chief Compliance Officer, is responsible for:

- Implementing and maintaining this Policy and related policies and procedures;
- Reviewing and refreshing the Program, risk assessment and any relevant training materials at least annually, and more frequently as circumstances require;
- Overseeing the implementation of the Program, including providing guidance and direction to XRP II staff about the steps they need to take to implement the Program;
- Ensuring that the Company fully meets its BSA/AML and sanctions reporting requirements in a timely fashion, including designing appropriate controls and coordinating independent testing of their effectiveness;
- Reviewing any changes to BSA/AML-related laws, regulations, guidance or regulatory expectations in consultation with our regulatory advisors and outside counsel to ensure that the Company remains fully in compliance with its legal obligations and regulatory expectations;
- Promptly alerting executive management to any material issues of BSA/AML/OFAC non-compliance, and instituting and monitoring corrective action;
- Providing periodic reporting to executive management on the state of BSA/AML/OFAC compliance and any significant emerging issues; and
- Arranging and ensuring that independent testing takes place at least annually

Chief Compliance Officer (CCO)

The CCO of XRP II is responsible for:

- Presenting an updated BSA/AML OFAC Program and corresponding Risk Assessment, as well as AML Training materials to executive management for review and approval on a no less than annual basis;
- Reporting to Ripple Labs' Board of Directors annually on the approval of the BSA/AML/OFAC Program, the corresponding Risk Assessment, and all relevant AML Training materials by XRP II executive management;
- Regular consultation with regulatory advisors and legal counsel to ensure that XRP II's BSA/AML/OFAC Policy and Program remains current with applicable laws and leading industry standards;

ripple

3

XRP II, LLC
BSA/AML/OFAC Policy 2015

- Providing quarterly validation reporting to Ripple Labs' Board of Directors evidencing appropriate and comprehensive governance of the XRP II BSA/AML/OFAC Compliance Program; and
- Providing BSA/AML/OFAC training to Ripple Labs' Board of Directors on an annual basis, or more frequently if needed.

Chief Executive Officer (CEO)

The CEO of XRP II is responsible for:

- Promoting and implementing a strong culture of compliance;
- Ensuring that the Company appoints a suitably qualified BSA/AML Officer;
- Ensuring that all staff promptly report violations or potential suspicious activity through the escalation procedures described in this policy;
- Reviewing compliance reports and any compliance issues escalated to executive management, including mitigation plans;
- Reviewing periodic BSA/AML/OFAC compliance reports from the Head of BSA/AML; and
- Reviewing the results of independent testing and ensuring that appropriate mitigation action is taken, where indicated.

Company Employees

All Company employees are responsible for:

- Reviewing and understanding the BSA/AML/OFAC Policy;
- Helping detect and prevent the use of Company services for money laundering, the financing of terrorist activities or other illegal conduct, or for fraud or financial crimes, as provided in the Program and compliance controls;
- Attending regular training regarding the BSA/AML/OFAC Policy and Program;
- Helping to ensure ongoing compliance with the BSA/AML/OFAC Policy and
- Program.

÷· ripple

4

XRP II, LLC
BSA/AML/OFAC Policy 2015

THE POLICY

An effective BSA/AML/OFAC Program is essential to both achieving and demonstrating compliance with legal requirements. This BSA/AML/OFAC Program is updated on an annual basis, or more frequently should circumstances warrant, and is presented annually by the Chief Compliance Officer to executive management for review and approval. The Chief Compliance Officer is also responsible for reporting to Ripple Labs' Board of Directors on the annual approval of the BSA/AML/OFAC Program by XRP II executive management. An overview of the policy is as follows:

Registration and Relationships

The Company maintains a registration as a money transmitter with FinCEN. At the time of this policy, the Chief Compliance Officer, in consultation with legal counsel, has determined that the Company is not subject to state licensing as a result of its activities. The Head of BSA/AML has responsibility for monitoring the need to apply for state licenses as a result of future changes to the Company's business

The Company does not have agents and will not establish any agency relationships.

Annual Risk Assessment

The BSA/AML/OFAC risk assessment identifies XRP II's BSA/AML and OFAC risks and assesses controls the Company has implemented to meet the regulatory expectations for money service businesses. The Head of BSA/AML conducts the risk assessment process including:

- Rating the inherent risk of XRP II's products and services, its customer base and the geographies in which its customers are located;
- Identifying and assessing the adequacy of XRP II controls in light of the BSA/AML and OFAC requirements for money transmitters registered with FinCEN;
- Rating the Company's residual risk in consideration of assessed controls; and
- Identifying and assigning responsibility for any necessary control enhancements identified as a result of the risk assessment process.

The Head of BSA/AML updates the Company's risk assessment on an annual basis. The updated risk assessment is presented annually by the Chief Compliance Officer to executive management of XRP II for review and approval. Additionally, the Chief Compliance Officer is responsible for reporting to Ripple Labs' Board of Directors on the approval of the annually updated risk assessment by executive management of XRP II.

Identification, Verification and Screening, and Know Your Customer

The Company employs customer identification procedures to verify the identities of our customers, screens customer names to ensure that they are not subject to OFAC sanctions, and conducts appropriate customer due diligence, including obtaining expected transaction activity, source of funds information as well as information regarding products and services offered by the customer.

5

RPLI_SEC 0095325

XRP II, LLC
BSA/AML/OFAC Policy 2015

The Head of BSA/AML, or designee, reviews all potential customers prior to onboarding and rejects customers that the company cannot adequately verify are subject to OFAC sanctions, or otherwise pose unacceptable BSA/AML risks.

Monitoring, Reporting, and Information Disclosures

The Company monitors its services for suspicious activity and reports this activity as required by law. In addition to filing suspicious activity reports ("SARs"), law enforcement is notified of any cases that specific agencies may have particular interest in. The Company also responds as appropriate to requests for information from FinCEN and other governmental entities, and, when appropriate, undertakes voluntary information sharing as provided in 31 C.F.R. § 314(b)

Testing of Controls

In addition to conducting routine internal testing, the Chief Compliance Officer and/or Head of BSA/AML regularly consults with our regulatory advisors and legal counsel to ensure that our BSA/AML/OFAC Policy and Program stays current with applicable laws and leading industry standards.

Training and Education

The Head of BSA/AML is responsible for ensuring that employees receive appropriate training on the requirements of the Company's BSA/AML/OFAC Policy and Program. The Chief Compliance Officer is responsible for providing BSA/AML/OFAC training to Ripple Labs' Board of Directors on an annual basis, or more frequently if needed. All relevant training materials must be approved by XRP II executive management on an annual basis. Evidence of approval is then reported annually to Ripple Labs' Board of Directors by the Chief Compliance Officer annually. Records of approvals are maintained centrally by the XRP II Compliance team.

Management Reporting

The Head of BSA/AML prepares BSA/AML Compliance Reports on a quarterly basis for executive management of XRP II and the Board of Directors of XRP II's parent company, Ripple Labs. This report describes key BSA/AML Program activities and reports on key risk indicators such as changes to XRP II's customer base, size and number of transactions, as well as any identified instances of suspicious activity, fraud or other wrongdoing.

The Chief Compliance Officer is also responsible for providing quarterly validation reporting to Ripple Labs' Board of Directors evidencing appropriate and comprehensive governance of the XRP II BSA/AML/OFAC Compliance Program.

❖ ripple

6

XRP II, LLC
BSA/AML/OFAC Policy 2015

Recordkeeping

The Company maintains records of customer identities, suspicious activity investigations, reports, and disclosures of information in response to governmental requests. Additional records, as required by law, are also created and maintained.

REGISTRATION AND RELATIONSHIPS

Money Transmission, Licensing and Registration

The Head of BSA/AML is responsible for ensuring that the Company registers as a MSB with FinCEN and maintains the Company's federal registration and renewal as required by law. The Head of BSA/AML, is also responsible for determining whether Company is required to obtain a money transmission license or other money services license in a particular state. The Company retains all documents regarding MSB or other money transmitter registration and state licensure indefinitely.

Agency Relationships

The Company does not have agents and will not establish any agency relationships

Banking Relationships

It is XRP II's intention to fully cooperate with all bank partner requests, as legally permitted, during partner bank's regulatory reviews and to cooperate insofar as possible with bank compliance oversight, as necessary.

Foreign Bank Account Registration

The Company does not have any foreign bank accounts and will not establish any foreign bank accounts.

Notice of information Sharing

The Company has notified FinCEN that XRP II elects to share information pursuant to section 314(b) of the USA Patriot Act. The Head of BSA/AML, or appointed designee, will renew the notice on an annual basis, as appropriate.

A copy of any form or notice submitted and all associated documentation related to the filing of the notice, including the content of any information shared with another financial institution is retained for a period of five (5) years.

ripple

7

XRP II, LLC
BSA/AML/OFAC Policy 2015

BSA/AML/OFAC PROGRAM

RISK ASSESSMENT

The BSA/AML Officer conducts a BSA/AML/OFAC risk assessment for XRP II on an annual basis. The purpose of the risk assessment is to identify XRP II's BSA/AML and OFAC risks, and assess controls XRP II has implemented to meet the regulatory expectations for an MSB. The risk assessment forms the basis of the annual BSA/AML Program, and will.

- Identify the Company's risk profile, by assessing the inherent risks presented by XRP II's products and services, customer base and the geographies in which it or its customers operate.
- Determine the adequacy and effectiveness of Company's controls;
- Identify the existence of any insufficiently mitigated risk; and
- Recommend any necessary enhancements to the BSA/AML/OFAC Compliance Program needed to reduce residual risk to an acceptable level. From time to time, as part of the risk assessment the Head of BSA/AML may recommend particular leading practice enhancements for certain BSA/AML/OFAC controls, as deemed appropriate.

INTERNAL CONTROLS

Customer Identification Program ("CIP") and Know Your Customer ("KYC") Activities

XRP II carries out its CIP and KYC programs as follows: XRP II collects customer identification information and verifies that information before permitting a customer to conduct an initial transaction, and on an ongoing basis as necessary or required by law. Due to the high inherent BSA/AML risk associated with virtual currency, the Company conducts additional due diligence on all of its customers. The Company also conducts the following screenings: sanctions screening; politically exposed person ("PEP"); negative news, and a general internet search for other potential risk factors.

Compliance personnel working under the direction of the Head of BSA/AML undertake the KYC process, using the forms attached as Appendix A to this policy.

Identification requirements for individuals

To purchase XRP from the Company, an individual customer must provide:

- o Full legal name;
- o Physical Address;
- o Date of Birth;
- o Tax payer identification number (TIN) such as a social security number or other government-issued identification number acceptable to the Head of BSA/AML; and
- o Copy of a valid, government-issued photo identification card such as a driver's license or passport
- o Copy of a photo of the individual holding their ID such that the person's face and picture on the ID are visible to the camera

Identification requirements for entities

To purchase XRP from the Company, an entity customer must provide:

ripple

8

XRP II, LLC
BSA/AML/OFAC Policy 2015

- o Names of the party, beneficial owners, officers and directors, and subsidiaries and controlled affiliates;
- o Physical Address.
- o Taxpayer Identification Number (TIN);
- o A list of all beneficial owners or ultimate beneficial owners with 25% or more ownership;
- o Copy of a document evidencing the legal existence of the entity, such as articles of incorporation or association[1]; and
- o Copy of a valid, government-issued photo identification for all persons with 25% or more beneficial ownership in the entity.
- o Copy of a photo of all persons with 25% or more beneficial ownership holding their ID visible to the camera.
- o Proof of address or existence of physical location of the entity

Verification procedures

The Head of BSA/AML, or compliance personnel working under her direction, review for inconsistencies in the information provided by the customer, and consider documentary evidence, non-documentary evidence or both to verify a customer's identity.

In the first instance, the Head of BSA/AML or compliance personnel working under her direction, make use of available documentary evidence to verify customer identity. Compliance personnel may also use non-documentary means such as online verification services to verify customer identity if:

> (1) compliance personnel are unfamiliar with any documents presented; or
> (2) the Head of BSA/AML believes it will provide greater assurance about the identity of the customer.

The Company will not conduct business with a customer who does not provide identification information. If a potential or existing customer refuses to provide all requested CIP and KYC information or appears to have intentionally provided misleading information, the Company will not conduct any further transactions with the customer. In such circumstances, the Head of BSA/AML will determine whether to file a SAR.

If the Company cannot verify the true identity of a potential customer to the satisfaction of the Head of BSA/AML, she will:

- o Ensure that Company does not conduct any transactions with that individual or entity, or otherwise establish a customer relationship; and
- o Determine whether to file a SAR.

The Company documents its customer identification and verification, including all identifying information, the methods used and results, and the resolution of any discrepancies. The Company will keep records containing a description of any document relied on to verify a customer's identity, noting the type of document, any identification number in the document, the place of issuance, and if any, the dates of issuance and expiration. With respect to non-documentary verification, the Company will retain documents that describe the methods and the results of any measures it took to conduct such verification.

---

[1]

For all articles of incorporation and identity verification documentation presented that is not in English, it is the responsibility of the customer to provide a third party translation. With the exception of proof of address, which may be a utility bill, lease agreement, or other document with the customer's name and address, XRP II will not accept documentation in a language other than English.

9

XRP II, LLC
BSA/AML/OFAC Policy 2015

The Company will retain records of required identification obtained at account opening for the duration of the customer relationship and for five (5) years after the customer account is closed (or five (5) years after the last transaction undertaken by the customer).

OFAC Compliance and Section 311 Screening

The Company screens both individual and entity customers, in addition to all XRP II employees, against the OFAC SDN list and on the FinCEN special measure entities list prior to onboarding. The Company screens new customers against OFAC's SDN list and jurisdictions subject to broad OFAC sanctions, as well as list of special measure entities, jurisdictions and transactions provided by FinCEN. The Company will not conduct any transactions, or otherwise establish a customer relationship, with any individuals or entities subject to OFAC sanctions.

Due to the relatively small number of customers and few transactions, the Head of BSA/AML or compliance personnel working under her direction, rescreens active[2] customers monthly. For existing customers, the Head of BSA/AML, or designee, must sign off on updated forms every time a customer transacts, unless the transaction is within one month of a previous transaction or is consistent with past customer activity. Designated compliance staff review all XRP II transactions on a quarterly basis to confirm/validate this activity. All potential OFAC hits must be referred to the Head of BSA/AML, except in circumstances where procedures specifically authorize other staff to resolve obvious false positives.

No staff member will conduct any transactions with any individual or entity under review for possible OFAC matches.

Politically Exposed Persons (PEPs)

When evaluating potential XRP II customers, the Head of BSA/AML, or appointed designee, conducts comprehensive screening to determine whether the potential customer is a known PEP. PEPs are generally defined as:

- A "**senior foreign political figure**" is a senior official in the executive, legislative, administrative, military or judicial branches of a foreign government (whether elected or not), a senior official of a major foreign political party, or a senior executive of a foreign government-owned corporation. In addition, a senior foreign political figure includes any corporation, business, or other entity that has been formed by, or for the benefit of, a senior foreign political figure.

- The "**immediate family**" of a senior foreign political figure typically includes the figure's parents, siblings, spouse, children, and in-laws.

- A "**close associate**" of a senior foreign political figure is a person who is widely and publicly known to maintain an unusually close relationship with the senior foreign political figure, and includes a person who is in a position to conduct substantial domestic and international financial transactions on behalf of the senior foreign political figure.

---

[2] An "active" customer is defined as one that has conducted any transaction within the prior rolling six month period.

XRP II, LLC
BSA/AML/OFAC Policy 2015

XRP II considers all PEPs to be high risk and subject to annual compliance reviews. Upon identification of a PEP, in addition to obtaining a completed KYC, designated XRP II compliance staff will request and review information concerning:

- the potential customer's background, income sources, source of funds and wealth and any other financial information deemed appropriate;
- the purpose of the account(s) and expected volume and nature of account activity;
- any immediate family members or close associates with transaction authority over the account or benefitting from transactions conducted through the account.

At this time, XRP II has identified no PEP customers. If an existing customer is subsequently identified as a PEP, through ongoing PEP screening of active customers, all relevant risks will be evaluated and appropriate action taken at that time.

Shell Companies

The term "shell company," refers to non-publicly traded corporations, limited liability companies (LLCs), and trusts that typically have no physical presence (other than a mailing address) and generate little to no independent economic value. Most shell companies are formed by individuals and businesses for legitimate purposes, such as to hold stock or intangible assets of another business entity or to facilitate domestic and cross-border currency and asset transfers and corporate mergers. Shell companies have become increasingly common tools for money laundering and other financial crimes, primarily because they are easy and inexpensive to form and operate.

Because shell companies can obscure company structure, ownership, and activities, XRP II considers them to be high risk entities. Shell companies that issue bearer shares are prohibited from conducting business with XRP II. When assessing the risk of shell companies and shell company relationships, XRP II considers the ownership structure, nature of the customer, the services provided, the purpose of the account, the location of services, and other associated factors. Risks are appropriately and effectively identified and managed in accordance with XRP II AML Program requirements.

Monitoring Transactions for Suspicious Activity

The Company monitors all customer transactions for suspicious activity. Suspicious activity is activity that indicates the possibility of:

Due to the wholesale nature of its business and the relatively small number of transactions, all of XRP II's transactions are individually reviewed by the Head of BSA/AML or compliance personnel working under her direction. When warranted, this review can include assessment of the totality of transactions conducted by that customer and consistency of those transactions with the KYC information collected.

In addition, the Company requires all personnel to report unusual or potentially suspicious activity to the Head of BSA/AML..

ripple

11

RPLI_SEC 0095331

XRP II, LLC
BSA/AML/OFAC Policy 2015

In conducting transaction monitoring, the Head of BSA/AML, or compliance personnel working under her direction look for "red flags" that could indicate suspicious activity. Such red flags include, but are not limited to:
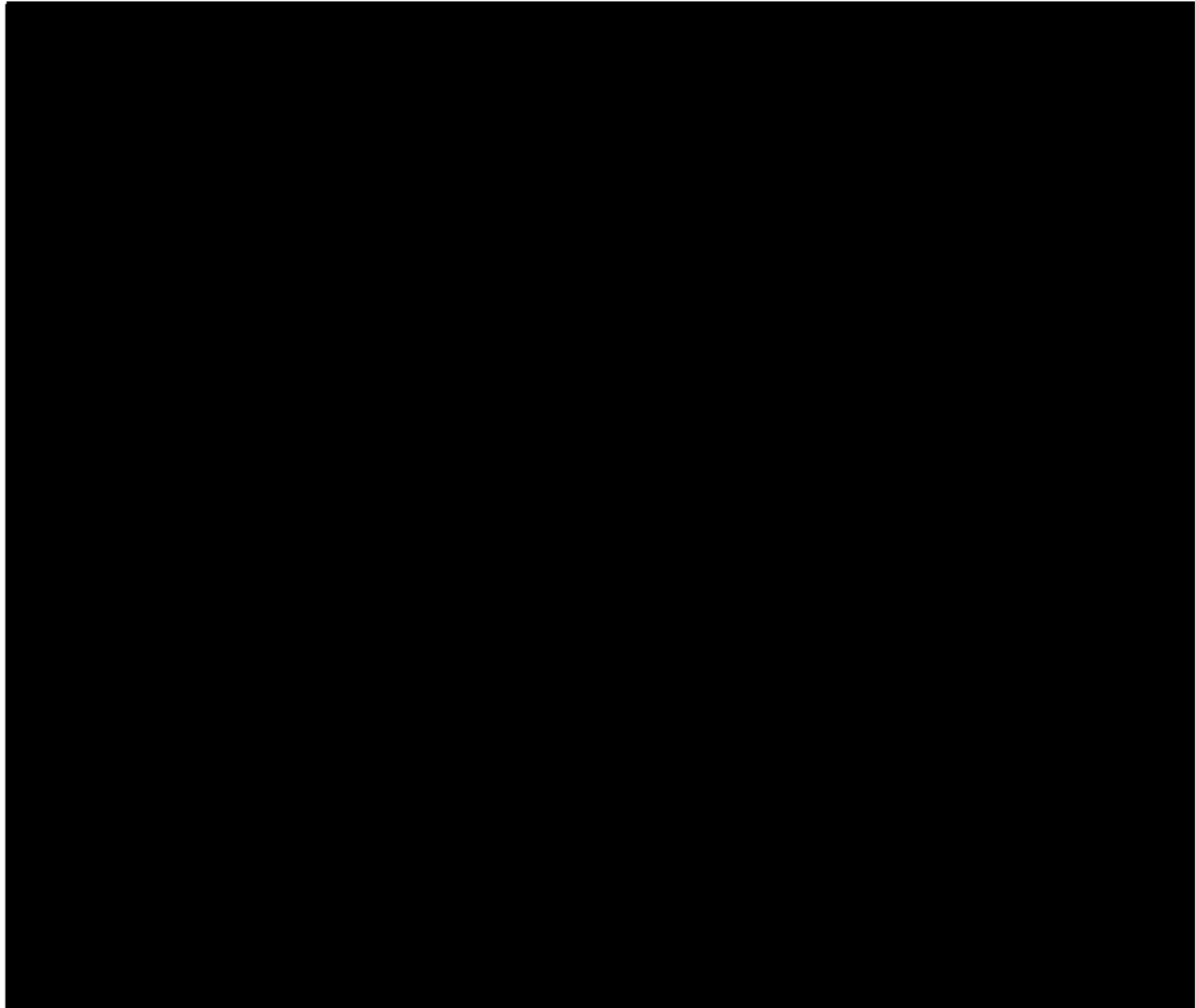
Suspicious Activity Investigations

Should the Compliance identify, or be notified of, suspicious activity or a red flag, the Head of BSA/AML will initiate an investigation into the activity. The Head of BSA/AML, or designee, must fully document the investigation in writing, including all steps taken. If Head of BSA/AML determines that the activity in question is not suspicious, the reasoning behind this decision must be clearly documented in the investigation file.

12

XRP II, LLC
BSA/AML/OFAC Policy 2015

Reporting Suspicious Activity

The Head of BSA/AML, or appointed designee, will initiate the filing of a SAR if the amount of suspicious activity identified is over USD $████ and:
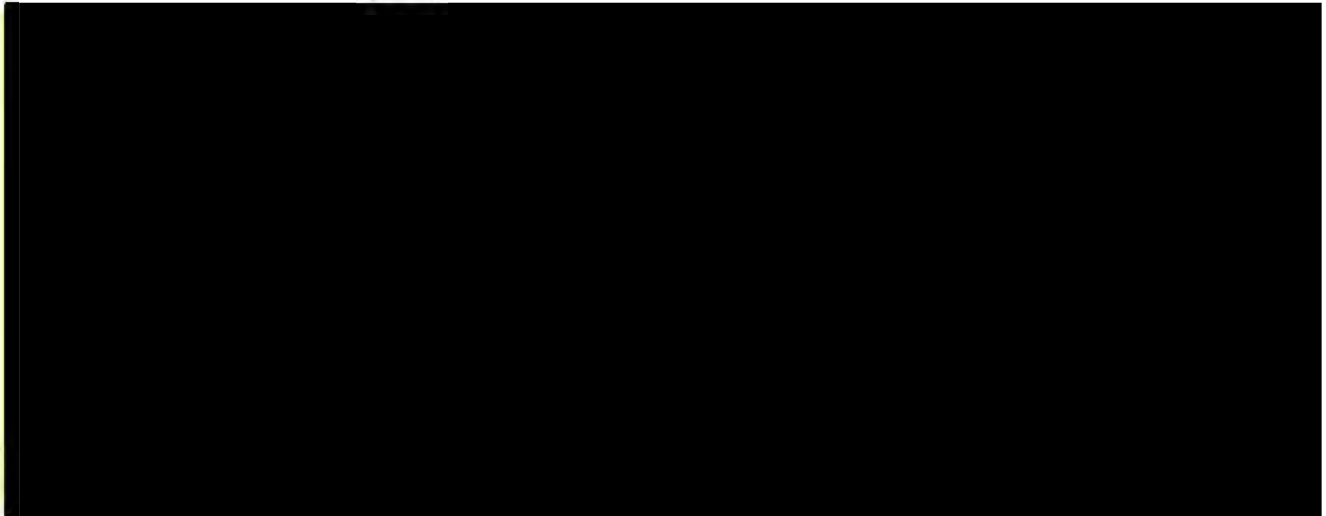
The Head of BSA/AML may choose to report the suspicious activity voluntarily if the transaction falls below the USD $████ monetary threshold in cases where a SAR may provide useful information to law enforcement. The Head of BSA/AML is responsible for the final determination regarding whether a report is required or will be voluntarily made.

The Head of BSA/AML is responsible for ensuring that the SAR is filed no later than 30 days after the determination that suspicious activity has occurred.

If the Head of BSA/AML determines that potential violations require immediate attention, such as in the case of ongoing money laundering, she will immediately notify by telephone the appropriate law enforcement agency, in addition to filing a SAR. Moreover, should the activity in question indicate the possibility of terrorist activity, the Head of BSA/AML will voluntarily report the activity to FinCEN, as appropriate.

Should the Head of BSA/AML determine that any of the following conduct is occurring, she will immediately notify Federal law enforcement by telephone

o   A customer account holder, or a person with whom such an account holder is engaged in a transaction, is listed on or located in a country or region listed on the OFAC list;
o   A customer account is held by an entity that is owned or controlled by a person or entity listed on the OFAC list;
o   A customer tries to use bribery, coercion, or similar means to open an account or carry out a suspicious activity.
o   The Company has reason to believe a customer is trying to move illicit cash out of the government's reach;
o   The Company has reason to believe a customer is about to use the funds to further an act of terrorism, engage in money laundering, or otherwise engage in illegal activity; or
o   The Company has other reasons to believe that one or more law enforcement agencies may benefit from direct notification of the suspicious activity.

13

RPLI_SEC 0095333

XRP II, LLC
BSA/AML/OFAC Policy 2015

SAR Follow-up:

In the event that a SAR is filed, the Head of BSA/AML will determine whether it is appropriate to terminate the customer relationship in question. This determination will be reached using a risk-based approach, taking into account the nature and location of the customer, the volume and size of the customer's transactions, and other relevant factors affecting the risk profile of the customer. The Head of BSA/AML is responsible for documenting the basis for the decision reached. When the customer relationship is not terminated, the Head of BSA/AML, or designee, will conduct a follow-up 90-day review to determine whether there is continuing activity that warrants an additional SAR filing.

Copies of all SARs filed and all supporting documents must be retained securely and confidentially for at least five (5) years after filing.

Maintaining the confidentiality of the SAR:

No officer, director, employee, agent, or service provider of Company may notify any person outside of the Company that any transaction or person has been reported in a SAR.

The Company prohibits all staff from "tipping off" users that they are under investigation or that Ripple Labs has filed a SAR naming them. The Head of BSA/AML ensures that all employees receive training (including the prohibition against "tipping-off") on how to report suspicious activity as part of the BSA/AML/OFAC training program, which is summarized below. To reduce risk of disclosure, the Company restricts internal access to SAR filings, documentation and other SAR-related information to the Head of BSA/AML, other compliance staff and executive management.

Currency Transaction Reporting

It is the policy of Company not to accept payment in the form of physical currency (i.e., the coin or paper of the United States or any other government).

Law Enforcement Requests

It is Company's policy to cooperate to the extent permitted by applicable law and in accordance with its policies, with legal process or other requests for information or assistance received from law enforcement.

The Head of BSA/AML reviews all requests for information or assistance from law enforcement, consults with legal counsel prior to disclosing any information to determine whether it is permissible to provide the requested information or assistance, and then responds accordingly to law enforcement.

Records of law enforcement legal process and requests, and productions made in response will be retained for five (5) years.

Records of law enforcement requests and productions are kept confidential and disclosed only:
- as allowed by the legal process;
- within the Company or to outside counsel as necessary to comply with the request;
- for legal advice; or to prepare a responsive production.

14

XRP II, LLC
BSA/AML/OFAC Policy 2015

National Security Letters ("NSLs")

All NSLs shall be referred to the Head of BSA/AML who consults with legal counsel prior to disclosing any information, and responds accordingly to law enforcement.

Records of NSLs and productions made in response will be retained for five (5) years.

NSLs must be treated with the highest levels of confidentiality, the existence of an NSL will be disclosed only as necessary to comply with the requests contained in it. Records of NSLs must also be kept confidential.

Voluntary Information Sharing (Section 314(b))

Should circumstances warrant, the Company may choose to undertake voluntary information sharing as provided in 31 C.F.R. § 314(b).). The Company has submitted a notification to FinCEN confirming its participation in this information sharing program. Any decision to share information pursuant to § 314(b) will be reached by the Head of BSA/AML in consultation with executive management and legal counsel. Information sharing under §314(b) must be limited exclusively to investigations of possible money-laundering or terrorist financing.

Before undertaking any voluntary information sharing, the Head of BSA/AML, or designee, must ensure that if the information is to be shared with the financial institution, that financial institution has filed the appropriate notice with FinCEN.

The Head of BSA/AML, or appropriate designated compliance staff, is responsible for handling all incoming § 314(b) requests. The Head of BSA/AML must authorize all outgoing § 314(b) requests. Should the Company receive information shared pursuant to § 314(b), the Head of BSA/AML will ensure that the information is used only for the following purposes:

  o   Identifying and, where appropriate, reporting on money laundering or terrorist activities;
  o   Determining whether to establish or maintain an account, or to engage in a transaction; or
  o   Assisting the sharing financial institution in complying with performing such activities.

If the shared information reveals suspicious activity, the Head of BSA/AML will initiate an investigation that may result in the filing of a SAR in accordance with this policy.

Records of information sharing and information received will be retained for five (5) years. Any such records must be maintained confidentially and securely.

XRP II, LLC
BSA/AML/OFAC Policy 2015

TESTING OF CONTROLS

Independent Auditing of Policy and Program

The Head of BSA/AML will identify a qualified, independent third party to conduct testing of the Company's BSA/AML/OFAC controls on an annual basis.

Annual testing will include an audit of Company's compliance with its own BSA/AML/OFAC Program. The audit must include, at a minimum:

- o Evaluation of the overall integrity and effectiveness of Company's BSA/AML Program;
- o Testing of all affected areas to ensure compliance with the BSA/AML Program;
- o Reviewing the flow of funds and the scope of Company's business to determine whether additional compliance controls should be added to the BSA/AML/OFAC Program;
- o Reviewing exception items to the BSA/AML/OFAC Program;
- o Reviewing the process for referring, investigating and reporting suspicious activity and "red flags";
- o Sampling of transactions for compliance, with an emphasis on high-risk transactions;
- o Reviewing and testing compliance for recordkeeping and record retention policies;
- o Reviewing and testing procedures for OFAC screening and customer and identification and verification (KYC);
- o Evaluating the Company's response to any previously identified deficiencies;
- o Reviewing adequacy of the training program; and
- o Reviewing of Program controls.

The auditor will issue a report of its findings upon completion of its audit to executive management. The report must include any deficiencies and recommendations for enhanced compliance, including any recommended changes to the BSA/AML/OFAC Policies or Program. The Head of BSA/AML will create and implement a remediation plan to address each of the resulting recommendations, as appropriate.

Records of independent testing must be retained for at least five (5) years.

TRAINING AND EDUCATION

The Head of BSA/AML ensures that the Company's personnel receive appropriate BSA/AML training.

Training will include a review of this BSA/AML/OFAC Policy and program, as well as a discussion of the following, with sufficient detail to allow each person receiving the training to perform his or her job function.

- o The Company's responsibilities for compliance under the BSA, the USA PATRIOT Act, the OFAC statutes and regulations, and any other applicable laws, including specific program controls;
- o Designated roles in the BSA/AML/OFAC Program;
- o The function and of the Head of BSA/AML;
- o Any recent changes to regulations or internal processes and controls;
- o How to identify red flags and signs of suspicious activity and what to do when risks are identified;
- o The Company's record-keeping and document retention policies; and
- o Consequences to the Company and to individuals for non-compliance, including statutory penalties and internal discipline/penalties.

⟪ ripple

16

RPLI_SEC 0095336

XRP II, LLC
BSA/AML/OFAC Policy 2015

Trainees must receive initial training within thirty days of joining the Company, if feasible, and at least annually thereafter, and/or when significant changes to the law/BSA/AML Program/XRP II warrant.

The Head of BSA/AML, or designated compliance staff, is responsible for retaining records for at least five (5) years from the date of training for each trainee.

ISSUE ESCALATION

Issue Escalation

One of the primary means for the Company to detect suspicious activity is through information provided by staff members most familiar with its customers. Employees are encouraged to bring any anomalous behavior to the attention of their management. In addition, it is the responsibility of all Company employees to be alert and to report to the Head of BSA/AML unusual or questionable activity by customers, in customer accounts, or related to transactions occurring through the Company. Employees are urged to be vigilant at all stages of the client acceptance process and thereafter during the life of the client relationship.

Any Company employee who observes suspicious activity or any of the red flags described above must immediately report the suspicious activity to the Head of BSA/AML. If possible, the referral should include identifying information for the customer or recipient, the details of the transaction, information about any other financial institution involved, and the basis for suspecting illegal activity.

Internal Reporting of Unusual Activity

The Company has established an internal Unusual Activity Reporting (UAR) process governing the receipt and processing of employee reports of unusual activity or suspected non-compliance with the Company BSA/AML/OFAC Program. If an employee has reason to believe that certain activity may be suspicious in nature, the employee must complete a UAR and submit it to the compliance team for further investigation and possible SAR filing. Only designated compliance staff members have access to UARs submitted by Company employees. UARs are maintained securely for a period of five (5) years from the date of employee submission (or from the date of SAR filing, if warranted).

Anonymous Reporting

Should a Company employee wish to report suspicious activity or non-compliance with this BSA/AML/OFAC Program anonymously, he or she may do so using the Company's confidential reporting service, accessible via phone at 855.874.2657 or online at www.ripplelabs.ethicspoint.com.

The Head of BSA/AML, or a designated compliance staff member, has access to the email inbox or voicemail and are responsible for keeping reports strictly confidential, disclosing only the suspected activity and not the name of the individual who submitted the report, and only as necessary to implement the BSA/AML/OFAC Program.

Correcting Program Violations

The Head of BSA/AML will take appropriate measures to correct any violations of this BSA/AML/OFAC Program. Regarding internal violations of the Program, the Head of BSA/AML will consult with

17

RPLI_SEC 0095337

XRP II, LLC
BSA/AML/OFAC Policy 2015

appropriate personnel within the Company to ensure that appropriate corrective action is taken in accordance with the applicable employment or other internal Company policy(ies).

With respect to violations of the BSA/AML/OFAC Program by external service providers, agents or subcontractors, the Head of BSA/AML will consult with the appropriate Company business and legal personnel to take appropriate action in accordance with the applicable agreement with the entity.

Records of corrective action shall be retained for at least five (5) years, or longer if required by the laws implicated in the corrective action (for example, by employment or contract law).

MANAGEMENT REPORTING

Quarterly BSA/AML Compliance Reports

The Head of BSA/AML prepares BSA/AML Compliance Reports on a quarterly basis for executive management of XRP II. The BSA/AML Compliance Report for XRP II describes key BSA/AML Program elements and activities and reports on key risk indicators such as changes to XRP II's customer base, size and number of transactions, as well as any identified instances of fraud or other wrongdoing.

Quarterly BSA/AML Compliance reporting to XRP II executive management may include:
*   regulatory compliance and MSB updates related to Virtual Currency;
*   recent global money laundering enforcement actions;
*   state regulatory reporting and licensing updates;
*   examinations and audit reviews;
*   training, compliance staffing, and technology resource needs;
*   SARs filed;
*   bank relationship status; and,
*   any other relevant required regulatory reports.

Reports of International Transportation of Currency or Monetary Instruments ("CMIRS")

The CMIRs requirements do not currently apply to XRP II because the Company does not transport, mail or ship currencies or monetary instruments within the IRS and Treasury's definition of currency and negotiable instruments.

If, due to a change in definitions or XRP II's business activities, the Company determines that it will accept currency or negotiable instruments as defined by the agencies, the Head of BSA/AML will amend this Policy/Program and develop procedures for filing CMIRs in accordance with the relevant regulations.

Funds Transmittal Recordkeeping

With respect to any single transaction or aggregated series of transactions from one individual or multiple individuals known to be acting in concert totaling more than USD $3,000 in a single day, the Company will collect and retain the following records:

    o   The name and address of the customer;

ripple

18

XRP II, LLC
BSA/AML/OFAC Policy 2015

- o   The amount of the order;
- o   The execution date of the order;
- o   Any payment instructions received from the customer;
- o   As many of the following received with the order: the name and address of the recipient, the account number of the recipient, or any other specific identifier of the recipient; and

Any form relating to the order that is completed or signed by the customer placing the order.
When the Company is the transmitter of a transmittal order of USD $3,000, it provides to the customer, at the time it sends the order to the receiving destination, the following information

- o   The amount of the order;
- o   The execution date of the order;
- o   The identity of the recipient's Ripple wallet; and
- o   Any other information deemed relevant to the order.

The Company retains the records of subject transactions for five (5) years.

POLICY VARIANCES

Any deviation from the requirements of this Policy must be first approved by the Head of BSA/AML. Approval may be granted in limited circumstances and cannot be granted indefinitely. The requestor must submit a written request to the Head of BSA/AM outlining the reason(s) for the variance, the time frame for the requested variance, and the replacement controls identified to mitigate the associated risk. The Head of BSA/AML, or designee, is responsible for tracking, maintaining and managing, all approved Policy variances.

POLICY ADMINISTRATION

The Head of BSA/AML reviews and updates the BSA/AML/OFAC Policy and Program no less than annually (more frequently when changes to the law/BSA/AML/OFAC Program/XRP II warrant). The Head of BSA/AML consults with regulatory and legal advisors as necessary in conducting this annual review. Executive management of the Company review and approve the BSA/AML/OFAC Policy and Program annually.

This BSA/AML/OFAC Policy was approved by the Company's CEO and Chief Compliance Officer and becomes effective on May 1, 2015.

Questions or suggestions about this Program Policy should be forwarded to the Head of BSA AML, Antoinette O'Gorman, at antoinette@ripple.com.

ripple

19

RPLI_SEC 0095339

XRP II, LLC
BSA/AML/OFAC Policy 2015

APPENDIX A

I.   KYC Forms Individuals
II.   KYC Forms Non-Individuals
III. KYC forms Hedgefunds

 ripple

20

XRP II, LLC
2015 Customer On-boarding KYC Form – Individuals

To be filled out by reviewer

- ☐ World-Check search (OFAC, PEP, SDN, Section 311)
- ☐ ID verification
- ☐ negative news
- ☐ Internet search

Comments:

Name of Reviewer: _____

Position: _____

_____
Signature   Date

Reviewed and Approved:

_____
Signature Chief Compliance Officer   Date

ripple

1

XRP II, LLC
2015 Customer On-boarding KYC Form – Individuals

To be filled by Individual

In connection with Anti-Money Laundering and Know Your Customer procedures and due diligence, please return this form as soon as practicable:

Customer Information

Full name: _____

Title: _____

Date of Birth: _____

Street Address (no P.O. Box please) :

_____

_____

_____

Phone number: _____

Email: _____

Country of Citizenship: _____

Government Issued ID Number (Social Security Number for U.S., Passport Number for non U.S.)

_____

Reason for purchasing XRP

_____

_____

_____

ripple   2

XRP II, LLC
2015 Customer On-boarding KYC Form – Individuals

Please describe your source of funds for purchasing XRP and provide any relevant supporting documentation (examples may include evidence of earnings, tax returns, bank or brokerage statements etc.)

_____

_____

_____

Location and Nature of Operations

Brief description of employment or business

_____

_____

_____

Do you intend to resell XRP or distribute funds? If so, please describe the approximate number of clients and transactions you anticipate and provide information about the location of these operations:

_____

_____

_____

_____

_____

Ripple Wallet public address: _____

Documentation

Please provide the identification/verification specified in **Annex A** of this document. If you believe that you are exempt from the requirement to provide us with such information based on one of the specific exemptions specified in **Annex A**, please state your rationale below:

ripple

3

XRP II, LLC
2015 Customer On-boarding KYC Form – Individuals

The undersigned hereby certifies that the information contained herein and the information in connection herewith (including documentation specified in **Annex A**, which is attached hereto) is true and correct as of the date hereof.

_____

Name

_____

Signature   Date

Annex A

Type of Counterparty	Required Counterparty Information (Listed above in KYC form)	Required Verification Documentation (Please attach additional documents)
Individual	- **Name** - **Address and contact information** - **DOB** - **Social Security or Tax ID** - **Source of Funds** - **Brief description of employment or business and reason for purchasing XRP**	- **Copy of a valid government-issued photo identification card (such as a driver's license or passport)** - **Photo of customer holding the photo identification card such that identification card and customer's face is visible** - **Documentation of proof of physical address (such as a utility bill or lease agreement)**

ripple

4

XRP II, LLC

2015 Customer On-boarding KYC Form – Non-Individuals

To be filled out by reviewer:

Entity/Corporate body:

❏ World-Check search (OFAC, PEP, SDN, Section 311)
❏ negative news
❏ Internet search

Comments:

Beneficiaries:

❏ World-Check search (OFAC, PEP, SDN, Section 311)
❏ ID Verification
❏ Negative news
❏ Internet search

Comments:

Name of Reviewer: _____

Position: _____

_____
Signature   Date

Reviewed and Approved:

_____
Signature BSA Officer   Date

1

XRP II, LLC
2015 Customer On-boarding KYC Form – Non-Individuals

To be filled by Entity:

In connection with Anti-Money Laundering and Know Your Customer procedures and due diligence, please return this form as soon as practicable.

Customer Information

Please provide the names of the following (if you need more room, please attach a rider):

Name of Entity: _____

Additional "Doing Business As" names:

_____

Beneficial owners of 25% or more:

_____

_____

Names of your officers and directors:

_____

_____

Names of your subsidiaries and controlled affiliates (if applicable)

_____

_____

Business Information

Customer Type: (Refer to Customer Type List for scoring)

☐ Other Banks   ☐ Limited Liability Company   ☐ Fund or Fiduciary Entities   ☐ Trust
☐ Sole Proprietor   ☐ Partnership   ☐ Corporation - Not publicly listed
☐ Government Agency   ☐ Non-Profit Organization   ☐ Professional Association
☐ Corporation - Publicly listed entity with primary listing on FRB approved stock exchange

Taxpayer ID number or Corporate Registration Number

_____

RPLI_SEC 0095346

XRP II, LLC

2015 Customer On-boarding KYC Form – Non-Individuals

Does your company have a physical business presence in your country of incorporation?
❑ If so, please check the appropriate box and state the address:
❑ If not, please check the appropriate box and state the address for the principal place of business:

_____

_____

_____

Primary phone number (if any)

_____

Website (if any)

_____

Principal Point of Contact

Name: _____

Phone number: _____

Email Address: _____

List contact information for all beneficiaries with 25% or more ownership, including director(S) of the entity, partner(s)/member(s) of the entity, and managing executive of the entity. (If you need more room, please attach a rider)

Beneficiary 1

Full name: _____

Title: _____

Date of Birth: _____

Address: _____

_____

_____

Phone number: _____   Email: _____

⚭ ripple   3

XRP II, LLC
2015 Customer On-boarding KYC Form – Non-Individuals

Beneficiary 2

Full name: _____

Title: _____

Date of Birth: _____

Address: _____

_____

_____

Phone number: _____ Email: _____

Beneficiary 3

Full name: _____

Title: _____

Date of Birth: _____

Address: _____

_____

_____

Phone number: _____ Email: _____

Location and Nature of Operations

Brief description of nature of operations and reasons for purchasing XRP:

_____

_____

_____

4

XRP II, LLC
2015 Customer On-boarding KYC Form – Non-Individuals

List the countries in which you (including subsidiaries and controlled affiliates) have operations or offices:

_____

_____

_____

Do you (including subsidiaries and controlled affiliates have operations/offices in any of the following countries (or governments of these countries):

Burma	❏ Y ❏ N
Cuba	❏ Y ❏ N
North Korea	❏ Y ❏ N
Iran	❏ Y ❏ N
Sudan	❏ Y ❏ N
Syria	❏ Y ❏ N
Belarus	❏ Y ❏ N
Côte d'Ivoire	❏ Y ❏ N
Zimbabwe	❏ Y ❏ N
Libya	❏ Y ❏ N

Do you (including subsidiaries and controlled affiliates) have business or financial dealings that benefit or involve (directly or indirectly) any of the following countries (or governments of these countries):

Burma	❏ Y ❏ N
Cuba	❏ Y ❏ N
North Korea	❏ Y ❏ N
Iran	❏ Y ❏ N
Sudan	❏ Y ❏ N
Syria	❏ Y ❏ N
Belarus	❏ Y ❏ N
Côte d'Ivoire	❏ Y ❏ N
Zimbabwe	❏ Y ❏ N
Libya	❏ Y ❏ N

5

RPLI_SEC 0095349

XRP II, LLC
2015 Customer On-boarding KYC Form – Non-Individuals

Do you intend to resell XRP or distribute funds? If so, please describe:

1) The approximate number of clients and transactions you anticipate

_____

2) Information about the location of these operations

_____

3) Estimate of the dollar amount of XRP that you intend to purchase XRP from the Company

_____

4) Estimate the frequency (per month, or per year) that you intend to purchase XRP from the Company

_____

Ripple Wallet public address: _____

Please describe your source of funds for purchasing XRP and provide any relevant supporting documentation (examples may include accounts, bank statements etc.)

_____

_____

_____

_____

6

XRP II, LLC
2015 Customer On-boarding KYC Form – Non-Individuals

Documentation

Please provide the identification/verification information specified in **Annex A** of this document. If you believe that you are exempt from the requirement to provide us with such information based on one of the specific exemptions specified in **Annex A**, please state your rationale below·

On behalf of _____, its subsidiaries, and controlled affiliates, the undersigned hereby certifies that the information contained herein and the information provided in connection herewith (including documentation specified in **Annex A**, which is attached hereto) is true and correct as of the data hereof.

_____
Name

_____
Signature   Date

7

XRP II, LLC

2015 Customer On-boarding KYC Form – Non-Individuals

Annex A

Type of Counterparty	Required Counterparty Information (Listed above in KYC form)	Required Verification Documentation (Please attach additional documents)
Entity	- Name - List of persons with 25% ownership or benefits of the entity, and their contact information - Social Security or Tax ID - Source of Funds - Brief description of nature of operations and reason for purchasing XRP	A. Copy of document evidencing the legal existence of the entity (such as articles of association) B. Copy of a valid government-issued photo identification card for (i) all directors of the entity (ii) all persons with 25% or more beneficial ownership in the entity, (iii) a partner/member of the entity, and (iv) a managing executive of the entity C. A photo of each of individuals under "B." holding the photo identification card such that identification card and customer's face is visible D. D. Documentation of proof of physical address of business operations (such as a utility bill or lease agreement)

8

XRP II, LLC
2015 Customer On-boarding KYC Form – Hedge funds

CUSTOMER DUE DILIGENCE
HEDGE FUNDS, PRIVATE EQUITY FUNDS, VENTURE CAPITAL FUNDS, FUNDS OF FUNDS ("FUNDS")

This form should be used for instances where the customer is the Hedge Fund, not the Investment Manager (IM) or the Administrator.

Is this entity partially or wholly owned by a government or a government-owned entity?
□ yes
□ no

□ Hedge Fund/ Fund of Funds – (e.g. Established as exempt pursuant to Section 3(c)(7) of the Investment Company Act
□ Private Equity Fund
□ Venture Capital Fund
□ Other (please specify)_____

Is the fund regulated?   □ yes   □ no   If yes, please attach proof of regulation
Country where fund is regulated _____
Name of regulatory body: _____

Does the fund have an Investment Manager[1]?   □ yes   □ no
Is the Investment Manager regulated?   □ yes   □ no
If yes, name of regulatory body: _____
Is the Investment Manager registered?   □ yes   □ no
If yes, name of body: _____

Country of Incorporation (for Fund) _____
Country of Incorporation (for Investment Manager) _____

Country of Operation – Fund _____
Country of Operation – Investment Manager _____
Country of Operation – Administrator _____

I. CUSTOMER (FUND) IDENTIFICATION

1. Name of Fund (full Legal Name)

2. Registered Address for the Fund (Principal place of business, local office (PO Box is acceptable provided a physical address is also listed)):

If address is same as Investment Manager/Adviser, include Investment Manager/Adviser name below:

---

[1] Investment Managers, Investment Advisors or Plan Administrators are collectively "Investment Managers." If there are multiple investment managers, for purposes of CIP/EDD, use the primary investment manager or management companies.

ripple

RPLI_SEC 0095353

XRP II, LLC
2015 Customer On-boarding KYC Form – Hedge funds

II. INVESTMENT ADVISOR/MANAGER ("IM") INFORMATION[1]
*If the IM is an existing customer, please skip question III and refer to IM profile for details herein.
1. Does the Fund have an Investment Manager?   ☐ yes   ☐ no
2. Investment Manager (IM) Full Name (Full Legal Name, including "Doing Business As or Trading As"):
3. Primary Business Address
4. Is the Investment Manager regulated?   ☐ yes   ☐ no   If yes, Name of regulatory body: _____   Country: _____

III. CUSTOMER (FUND) VERIFICATION AND NOTIFICATION
1. **Please provide one form of primary and one form of secondary documentation from the list below**

Type	Verification	Date of Issuance
Primary (documentary)	Certificate of Incorporation or equivalent jurisdictional document (may be obtained from a government website such as Companies House or foreign equivalent approved by Compliance)	
Primary (documentary)	Signed Articles of Association/Organization or equivalent jurisdictional document	
Primary (documentary)	Private Placement Memorandum, Offering Memorandum or Prospectus (mandatory unless Family Office)	
Primary (documentary)	Signed General Partnership Agreement	
Primary (documentary)	Signed LLC Agreement	
Primary (documentary)	Signed Limited Partnership Agreement	
Primary (documentary)	Business Name Filing document such as Ficticious Name Certificate or Certificate of Trade Name (attach document)	
Primary (documentary)	Proof of Formation document from a government agency website. If in a foreign language, it must be accompanied by a translation or certification form signed by Country Compliance (sample to be provided). Website must be approved by Compliance as an acceptable form of verification.	
Secondary	Proof of registration with monetary authority, state or country of incorporation	
Secondary	Proof confirming existence on a regulator's website (includes SROs)	
Secondary	License from a Financial Authority under which the entity operates	
Secondary	Audited Financial Statements	
Secondary	Certificate of Good Standing (US only, state based documentation)	
Secondary	Government/Regulator issued Business License	
Secondary	Search confirming existence on approved government websites. Website must be approved by Compliance as an acceptable form of verification	

•⁏ ripple

XRP II, LLC
2015 Customer On-boarding KYC Form – Hedge funds

IV. FUND INFORMATION
1. Identify the structure of the fund (e.g. Master, Feeder, Blocker, Operating, etc.):
2. Date of Incorporation/Formation:
3. Country of Incorporation:
4. Internet website URL:

V. FINANCIAL INFORMATION
1. Approximate assets under management (AUM) in USD – (at least one must be answered). As of: MM/DD/YYYY □ $0 – $5,000,000   □ $5,000,000 – $10,000,000   □ $10,000,000 – $50,000,000 □ $50,000,000 – $100,000,000   □ $100,000,000 – $500,000,000   □ $500,000,000 – $1,000,000,000 □ $1,000,000,000 or greater □ Start up Fund, document that the fund is a start up and explain source of seed capital below:

VI. FUND ADMINISTRATOR (IF APPLICABLE)
1. Does the Administrator perform AML/KYC on the Funds investors?   □ yes   □ no
2. Name (Full Legal Name, including "Doing Business As or Trading As"):
3. Primary Business Address:
4. Telephone number
5. Internet website URL (if available):
6. Is the Administrator Regulated?   □ yes   □ no

ripple

XRP II, LLC
2015 Customer On-boarding KYC Form – Hedge funds

VII. ANTI-MONEY LAUNDERING QUESTIONNAIRE AND DUE DILIGENCE		
1. Does the Fund comply, either by itself or through its AML/KYC Service Provider, with the following:		
(a) Due diligence on fund investors, and, where appropriate, the ultimate beneficial owners of investors (for entity-investors)	☐ yes	☐ no
(b) The screening of investors against lists of persons, entities or countries sanctioned by the U.S. Treasury Department's Office of Foreign Assets Control or an applicable government/competent authority?	☐ yes	☐ no
(C) A prohibition against customers and transactions sanctioned by the U.S. Treasury Department's Office of Foreign Assets Control or other applicable government/competent authorities?	☐ yes	☐ no
(d) Document retention for fund investor due diligence	☐ yes	☐ no
(e) An internal audit function or other independent third party, other than government supervisors/regulators, that assesses AML/CTF policies and practices on a regular basis?	☐ yes	☐ no
(f) The identification of, and due diligence, and enhanced due diligence where appropriate, on investors that are Politically Exposed Persons (PEPs) their family, or close associates?	☐ yes	☐ no
(g) The identification, detection and reporting of suspicious activity where appropriate.	☐ yes	☐ no
(h) A policy prohibiting accounts/relationships with shell banks? (A shell bank is defined as a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group)	☐ yes	☐ no
(i) Training of key personnel with respect to anti-money laundering and sanctions compliance	☐ yes	☐ no
For any "no" answers, please provide and explanation:		

ripple

RPLI_SEC 0095356

XRP II, LLC
2015 Customer On-boarding KYC Form – Hedge funds

INTERNAL FACING:

II. CUSTOMER (FUND) VERIFICATION AND NOTIFICATION
Sources: Customer verification can be received either via public domain, email, faxed copy or hard-copy via post. Formation documents must be executed documents (unless company is in the process of being formed). Originals or certified copies are NOT mandatory. If formation or documents are not in English, a bank employee or other qualified individual must certify that the document provided is the appropriate document. A copy of the document certification form is attached in the Line of Business procedures.
Were any "substantive discrepancies" noted during the verification process? Substantive discrepancies would include the inability to verify entity name or an identification number; this must be escalated to Compliance for resolution. If the substantive discrepancy cannot be resolved, the account cannot be opened. Discrepancies not deemed to be substantive might include an inability to verify an address when other identifying information has been verified (such as might be the case in a recent change of address). All records related to the discrepancies made in the course of verifying identification of customers and how the discrepancy was resolved must be documented in the CDD and maintained for a period of five years from the date the record is made. If YES, identify the type of discrepancy and how substantive discrepancy was resolved: _____ If unable to resolve, [STOP COMPLIANCE MUST BE CONSULTED]]

OWNERSHIP AND SCREENING
1. Has the Fund been screened for OFAC, PEP status, Sanctions, internal watch lists, negative news, etc. in line with policy? ☐ yes   ☐ no
2. Were any material OFAC Sanctions, internal watch lists, and/or negative news matches identified? ☐ yes   ☐ no

V. REPUTATIONAL DUE DILIGENCE
1. Market reputation of the institution: Note and describe comments from other banks/bankers, media coverage, industry associastions, bank employees, reporting bureaus, rating services, or government industry reports with regard to whether the Fund or related businesses are experiencing any circumstances that could impact the reputation and/or viability of the Customer (considerations should include financial difficulties, industry/business investigation, government intervention, business/management reputational concerns) or if the fund has been subject to negative press, particularly with respect to money laundering matters.

X. REVIEW AND APPROVAL
To ensure that this customer is an appropriate customer for the bank, it is important that all information required herein has been obtained and that the information is accurate and that such information has been verified and corroborated.
CDD prepare by (Please Print Name) _____ Date: _____

ripple

XRP II, LLC
BSA/AML/OFAC Training and Education Program
June 2015

Training and Education Program Overview

XRP II, LLC ("XRP II" or "the Company"), its executive management, and its parent company's (Ripple Labs) Board of Directors are committed to ensuring that its products and services are not used to launder money, finance terrorism, evade U.S. Government sanctions or otherwise facilitate criminal activity. The Company's BSA/AML/OFAC Policy and Program sets forth XRP II's controls and compliance obligations with regard to Anti Money Laundering ("BSA/AML") and Sanctions rules and regulations.

The following BSA/AML/OFAC Training and Education Program describes XRP II's required training for employees and any other covered parties (including service provider personnel whose duties impact the Program as well as Ripple Labs directors) to ensure that sufficient training to comply with the provisions of BSA/AML and Sanctions rules and regulations in the course of his or her job function.

In addition to annual BSA/AML/OFAC training which all XRP II employees must complete, XRP II AML Compliance staff also attend additional internal and/or external training sessions, conferences and continuing education programs to remain current with AML and sanctions compliance requirements. The BSA Officer will also provide annual training to employees of Ripple Labs not covered by the XRP II Training Program whose job responsibilities may plausibly lead them to identify unusual activity involving XRP II users.

Roles and responsibilities

It is the responsibility of the BSA Officer to ensure that this Training and Education Program is adhered to and maintained. The BSA Officer is also responsible for informing senior management of any employees who do not appropriately follow the Company's BSA/AML/OFAC policy and/or fails to complete his or her training obligations in accordance with this Program. The status of XRP II employee BSA/AML/OFAC training is also reported by the BSA Officer to senior management on a quarterly basis, as applicable

A designated Compliance Analyst is responsible for documentation and record-keeping of attendance at internal BSA/AML/OFAC training sessions as well as recording of AML training certifications and any external BSA/AML/OFAC education and training sessions. All records are maintained in the 'Training' folder, within the XRP II AML Program files located on the Compliance designated secure server for a period of five years following the date of training or as specified in XRP II's Record Retention Policy: **rnc / XRP II AML / OFAC Program / 3-AML Procedures**

ripple Labs

XRP II, LLC
BSA/AML/OFAC Training and Education Program
June 2015

The XRP II AML Training folder is located here:
rnc / XRP II AML / OFAC Program / 7-AML Training Program / 2015 / Final

Schedule

All XRP II employees and any other covered parties are required to undergo annual BSA/AML/OFAC training. Any new XRP II employees and other covered parties will be required to undergo BSA/AML/OFAC training within thirty days of hire date.

It is the objective of the Company that as many XRP II AML Compliance employees as possible are CAMS (Certified Anti Money-Laundering Specialist) certified and receive ongoing BSA/AML/OFAC training opportunities. All AML Compliance employees are encouraged to attend external training events and webinars relevant to BSA/AML/OFAC compliance.

A tracking sheet of training sessions attended in 2015 to date is attached as **Exhibit B** to this document.

Annual Training

All XRP II employees and other covered parties, as applicable, are required to attend BSA/AML/OFAC training on an annual basis or more frequently, if warranted. XRP II's annual training covers:

- Company compliance responsibilities under the Bank Secrecy Act (BSA), the USA PATRIOT Act, Office of Foreign Assets Control ("OFAC" or, more broadly, "sanctions") regulations, and any other applicable AML laws;
- Specific XRP II AML/OFAC program controls;
- Designated roles in the AML/OFAC Program
- The function of the CCO/BSA Officer;
- Any recent changes to regulations and/or internal processes and controls;
- How to identify 'red flags' and indications of unusual activity and specific action to take when AML risks are identified;
- The Company's record-keeping and document retention policies; and

2

&rippleLabs

XRP II, LLC
BSA/AML/OFAC Training and Education Program
June 2015

- Consequences to the Company and to XRP II employees for non-compliance with AML/OFAC Program requirements, including statutory penalties and internal discipline/penalties.

The 2015 BSA/AML/OFAC Training presentation can be found here:
rnc / XRP II AML / OFAC Program / 7-AML Training Program / 2015 / Final

The attendance sheets for the 2015 AML Training sessions can be found here:
rnc / XRP II AML / OFAC Program / 7-AML Training Program / 2015 / Final

Supplementary Training

In addition to annual BSA/AML/OFAC training, XRP II AML Compliance staff, including the BSA Officer, must attend a minimum of ten (10) hours of internal or external Payments and/or AML-related education and training sessions. Attendance records at these sessions is documented and logged on an internal tracking list maintained by AML Compliance and saved in the XRP II AML Training Program folder located here:
rnc / XRP II AML / OFAC Program / 7-AML Training Program / 2015 / Final

BSA/AML/OFAC training records along with a roadmap for AML Compliance continuing education are tracked and documented by the AML Compliance team. A tracking sheet of training sessions attended throughout the year is attached as **Exhibit A** to this document.

A tracking sheet of training sessions attended by Compliance Personnel in 2015 to date is attached as **Exhibit B** to this document.

3

ᕼrippleLabs

XRP II, LLC
BSA/AML/OFAC Training and Education Program
June 2015

Exhibit A[1]: Annual AML Compliance Training for XRP II Employees

Date	Regulation/Opinion	Presenter	Present	Hours
02.26.2015	Annual AML Training			1
05.21.2015	Annual AML Training, for new XRP II employees			1
6.11.15	Make-up Annual AML Training session for senior management			1
6.16.15	Make-up Annual AML Training session for senior management			1

---

[1] Note: Additional annual AML training will be scheduled in the latter part of 2015 for remaining Ripple Labs employees and for Ripple Labs Board of Director members

4

rippleLabs

XRP II, LLC
BSA/AML/OFAC Training and Education Program
June 2015

Exhibit B: 2015 AML Compliance Training and Education Tracking List

Date	Regulation/Opinion	Presenter	Present	Hours
02.17.2015	Internal discussion on Draft EU Proposed AML Directive issued December 2014			1.5
02.23.2015	Global Monitoring Tool overview and training			1
02.26.2015	ACAMS Model and Validation Tuning			2
03.11.2015	Payments Training			2
03.15.2015	CAMS certification test prep, ACAMS, Florida			8
04.01.2015	Webinar: Lessons Learned From Recent Virtual Currency Cases			2
05.06.2015	Webinar: Effective SAR filing			2
05.21.2015	CAMS Certification Exam			N/A
06.01.2015	CAMS Certification Exam			N/A

5

rippleLabs

RPLI_SEC 0095362

Appendix 8 (Q32a/b) — Settlement Agreement and Remedial Measures

Settlement Agreement – Remedial Measures

Ripple Labs Update as of June 19, 2015

On May 4, 2015, Ripple Labs, Inc. ("the Company") and its wholly owned subsidiary XRP II entered into a Settlement Agreement with the Department of Justice and FinCEN. Ripple Labs is actively addressing required Remedial Measures as described in Attachment B to that Agreement.

The following outlines actions the Company has, or is, undertaking to develop or augment its BSA/AML/OFAC Compliance programs.

- Ripple Labs is committed to expanding its AML Compliance team with additional key hires over the coming months. Since 2014, Ripple Labs has hired an experienced Chief Compliance Officer, seasoned Legal Counsel, and a qualified Bank Secrecy Act Officer with 15 years banking and AML consulting experience.

- Per Settlement Agreement terms, Ripple Labs migrated its Ripple Trade wallet software to a Money Services Business ("MSB") and registered with FinCEN on June 2, 2015 (within 30 days of the Settlement date.)

- As a money services business, Ripple Trade is required to develop and implement an effective AML Program and conduct a comprehensive BSA/AML/OFAC risk assessment. Both were completed in early June and were approved/adopted by the Ripple Trade Compliance Oversight Committee on June 12, 2015.

- Ripple Labs has developed a customer identification ("CIP") 'tool' to assist with identification for Ripple Trade users. Effective June 2, 2015, Ripple Trade suspended onboarding new users until this functionality is in place. By October 30, 2015, Ripple will conduct CIP on users that existed prior to June 3, 2015 and will block access to the Ripple Trade service for any users that do not complete necessary CIP steps by that date. User identification information will be verified via non-documentary methods. The customer identification 'tool' will also be made available to other "gateways" on the Ripple protocol in support of our continued efforts to promote a healthy and compliant Ripple eco-system.

- Additionally, Ripple Labs developed and delivered required BSA/AML/OFAC training to all employees of Ripple Trade and XRP II within 45 days of the Settlement Agreement date. An effective AML training program and training schedule was already in place for XRP II, LLC; nonetheless, all XRP II employees received supplemental AML training. Training materials, attendance sheets, certifications, and AML Training Programs were delivered to outside counsel on June 18, 2015 for submission to both FinCEN and the United States Attorney's Office ("USAO").

1

RPLI_SEC 0095364

- Ripple Labs has also taken steps to improve existing analytical, monitoring, and reporting tools applicable to the Ripple protocol, as required within 60 days of the Settlement Agreement date. These improvements include: (a) risk rating of accounts; (b) enhancement of existing dynamic risk tools to facilitate investigation of suspicious activity, including counterparty reporting, flow of funds and degrees of separation analysis. Informal, third-party validation of global monitoring tool enhancements will commence during the week of June 22, 2015.

- In June 2015, Ripple Labs obtained requisite 'non-objection' from FinCEN and the USAO to secure and retain an external audit firm to examine its Ripple Trade and XRP II BSA compliance programs and evaluate their compliance with requirements of the BSA and associated regulatory rules applicable to money services businesses. Three detailed audit reviews, including comprehensive transaction reviews, will occur over the next five years, the first of which must be conducted within one year of the Settlement Agreement date.

- Within 180 days of the Settlement Agreement date, Ripple Labs is required to have completed a look-back review of all transactions to which Ripple Labs and/or XRP II was a party or served as an exchanger. Any suspicious activity identified as a result of this review will be reported to FinCEN, in accordance with BSA regulatory reporting requirements. To assist with this endeavor, in June 2015, Ripple Labs has engaged an independent, external consulting firm that specializes in transaction look-back reviews.

- On May 26, 2015, Ripple Labs submitted a request to FinCEN for an administrative ruling concerning the application of FinCEN's regulations implementing the Bank Secrecy Act, 31 C.F.R. Chapter X – in particular, the Funds Travel Rule and the Funds Transfer Rule, 31 C.F.R. §§ 1010.410(e)-(f) and, more specifically, their application to the Ripple Trade MSB entity given that Ripple Trade does not ever custody, hold, transfer, or control funds (in any currency, virtual or fiat). The request specifically seeks clarification on applicability for those transactions to which the Company, Ripple Labs, is *not* itself a party.

Antoinette O'Gorman

BSA Officer, Ripple Labs, Inc.

2